(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年3 月30 日 (30.03.2006)

PCT

(10) 国際公開番号
WO 2006/033266 A1

(51) 国際特許分類:
G06K 19/07 (2006.01) *G06F 1/30* (2006.01)

(21) 国際出願番号: PCT/JP2005/016849

(22) 国際出願日: 2005 年9 月13 日 (13.09.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-273023 2004 年9 月21 日 (21.09.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 谷川 諭 (TANIGAWA, Satoshi).

(74) 代理人: 新居 広守 (NII, Hiromori); 〒5320011 大阪府大阪市淀川区西中島３丁目１１番２６号 新大阪末広センタービル３Ｆ 新居国際特許事務所内 Osaka (JP).

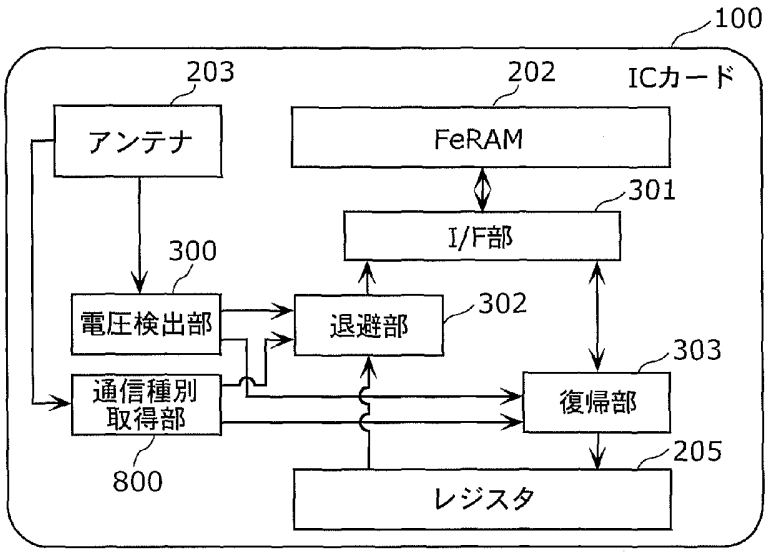
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

[続葉有]

(54) **Title:** SEMICONDUCTOR MEMORY CARD

(54) **発明の名称:** 半導体メモリカード



100 IC CARD
203 ANTENNA
300 VOLTAGE DETECTING PART
800 COMMUNICATION TYPE ACQUIRING PART
301 I/F PART
302 SAVING PART
303 RETURNING PART
205 REGISTER

(57) Abstract: A semiconductor memory card wherein even when the execution of a processing was interrupted due to an interruption of a voltage supply, the interrupted processing can be continuously executed after a voltage supply. The semiconductor memory card, which can execute programs, comprises a FeRAM for storing information; a register for storing information related to a program currently being executed; a voltage detecting part for detecting a variation of the voltage supplied to the semiconductor memory card; a saving part for associating the register information stored in the register with additional information, by which the program can be identified, and then saving these associated information into the FeRAM when the voltage detecting part detects a predetermined voltage drop; and a returning part for returning the register information to the register when the voltage detecting part detects a predetermined voltage rise and when the additional information stored in the FeRAM satisfies a predetermined condition.

[続葉有]

WO 2006/033266 A1

IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 本発明は、電圧の供給が中断することにより、処理の実行が中断される場合であっても、電圧の供給後に中断された処理を継続して実行することができる半導体メモリカードを提供する。 本発明の半導体メモリカードは、プログラムを実行可能な半導体メモリカードであって情報を格納するＦｅＲＡＭと、実行中のプログラムに関する情報を格納するレジスタと、半導体メモリカードに対する供給電圧の変化を検出する電圧検出部と、電圧検出部が所定の電圧低下状態を検出した場合、レジスタに格納されているレジスタ情報と、プログラムを特定するための付加情報とを対応付けてＦｅＲＡＭに退避させる退避部と、電圧検出部が所定の電圧上昇状態を検出した場合、ＦｅＲＡＭに格納されている付加情報が所定の条件を満たすとき、レジスタ情報をレジスタに復帰させる復帰部とを備える。

明 細 書

半導体メモリカード

技術分野

[0001] 本発明は、プログラムを実行可能な機能を有する半導体メモリカードに関する。

背景技術

[0002] 近年、クレジットカードをはじめ多くの磁気カードが半導体メモリカードへ転換されてきている。その理由として、半導体メモリカードは、磁気カードに比べて記憶容量が大きいことはもとより、格納される個人情報等の情報漏えいを防ぐセキュリティ機能が強化されていることが挙げられる。上記格納データの保護機能を持った半導体メモリカードの代表としてICカードがある。

[0003] ICカードには、ICカードとデータのやり取りを行なうリーダライタとの通信形態により接触型と非接触型とがある。非接触型ICカードとは、リーダライタが発信する弱い電波を利用してデータを送受信するICカードのことである。以下、単に「ICカード」という場合、非接触型ICカードのことを指すものとする。

[0004] 図1は、一般的なICカードのハードウェア構成の一例を示す図である。図1に示すICカードは、プログラムを格納するROM201、プログラム実行の際に用いられる一時的なデータや外部から書き込まれるデータを格納する不揮発性メモリであるFerroelectric Random Access Memory(FeRAM)202、外部との通信インターフェース(I/F)であるアンテナ203、および、ROM201に記憶されたプログラムに従って各種コマンド処理等の制御処理を行なうCPU200を備えている。

[0005] また、CPU200は、算術的な処理を行なう回路であるArithmetic and Logic Unit(ALU)204と、演算値や実行状態を保持する記憶素子であるレジスタ205とを有している。

[0006] ところで、このICカードは、従来、一枚のICカードに対し、電子マネー等の単純な単一のサービスの処理のみが要求されていた。しかし、近年の生体認証等による高度な認証技術の導入により、より複雑な処理を実行することが要求されている。複雑な処理を実行する場合、単純な処理を実行する場合と比べ、リーダライタとの通信を

継続する時間がより必要となる。

[0007] また、複数のサービスの処理が求められるため、近年のICカードでは、複数のサービスのそれぞれに対応する、複数のアプリケーションプログラム(以下、単に「プログラム」ともいう。)が実行可能となっている。ICカードは、サービスを提供するホストコンピュータであるサーバに接続されたリーダライタと通信を行なうことで、そのサーバが提供するサービスを利用することができる。

[0008] ここで、非接触型ICカードの特性として、リーダライタから発信される電波により電圧が供給されているため、ICカードをリーダライタから離すと、電圧の供給が遮断され、処理がリセットされることとなる。

[0009] そのため、電圧の供給が不安定な環境において、処理を継続する方法として、レジスタ、RAMを全て不揮発性メモリFeRAMで構成し、電圧の再供給後に、処理を再開する方法がある。

発明の開示

発明が解決しようとする課題

[0010] しかしながら、レジスタやRAM、特にレジスタのように、アクセス頻度の高い箇所に不揮発性メモリFeRAMを用いることは、FeRAMの特性上、商品寿命が極端に短くなるため商品化は現実的ではない。

[0011] また、ICカードは、上述のように、複数のサービスそれぞれに応じた処理を実行することが可能であり、電圧の供給の中断前と再開後で、ICカードが処理すべき内容が異なる場合がある。そのため、レジスタであるFeRAMに保持されていた演算値等をそのまま用いて処理を再開することができない場合がある。

[0012] 本発明は、上記課題を解決するものであり、電圧の供給が中断することにより、処理の実行が中断される場合であっても、電圧の供給後に中断された処理を継続して実行することができる半導体メモリカードを提供することを目的とする。

課題を解決するための手段

[0013] 上記従来の課題を解決するために本発明の半導体メモリカードは、プログラムを実行可能な半導体メモリカードであって、情報を格納する不揮発性メモリと、実行中のプログラムに関する情報を格納するレジスタと、前記半導体メモリカードに対する供給

電圧の変化を検出する検出部と、前記検出部が所定の電圧低下状態を検出した場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避部と、前記検出部が所定の電圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰部とを備える。

[0014] また、本発明の半導体メモリカードは、更に、他の機器と通信する通信部を備え、前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記付加情報が、前記通信部と前記他の機器との通信により得られた情報を含むとき、前記レジスタ情報を前記レジスタに復帰させるとしてもよい。

[0015] また、本発明の半導体メモリカードは、更に、前記通信部と前記他の機器との通信における通信種別を示す情報を取得する通信種別取得部を備え、前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記付加情報が、前記通信種別取得部により取得された前記通信種別を示す情報を含むとき、前記レジスタ情報を前記レジスタに復帰させるとしてもよい。

[0016] また、本発明の半導体メモリカードにおいて、前記不揮発性メモリは、互いに異なる複数のレジスタ情報を格納し、前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記通信種別取得部により取得された前記通信種別を示す情報を含む付加情報に対応付けられたレジスタ情報を、前記不揮発性メモリの中から選択して読み出し、前記レジスタに復帰させるとしてもよい。

[0017] また、本発明の半導体メモリカードにおいて、前記退避部は、前記レジスタ情報を前記不揮発性メモリに退避させる際に、更に、前記プログラムが利用する暗号の強度を示す暗号情報を前記レジスタ情報と対応付けて前記不揮発性メモリに退避させ、前記半導体メモリカードは、更に、他の機器と通信する通信部と、前記復帰部が前記レジスタ情報を前記レジスタに復帰させる前に、前記暗号情報に示される暗号の強度が所定の強度以上であるか否かを判断する復帰判断部と、前記復帰判断部が、前記暗号情報に示される暗号の強度が所定の強度以上であると判断した場合、前記他の機器の認証を行なう認証部とを備え、前記復帰部は、前記検出部が所定の電

圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たし、かつ、前記認証部による前記他の機器の認証が成功したとき、前記レジスタ情報を前記レジスタに復帰させるとしてもよい。

[0018] また、本発明の半導体メモリカードにおいて、前記不揮発性メモリは破壊読出し領域を有し、前記半導体メモリカードは、更に、前記退避部が前記レジスタ情報を前記レジスタに退避させる前に、実行中のプログラムが利用する暗号の強度が所定の強度以上であるか否かを判断する退避判断部を備え、前記退避部は、前記検出部が所定の電圧低下状態を検出した場合、前記退避判断部により前記暗号の強度が所定の強度以上であると判断されたとき、前記レジスタ情報と前記付加情報とを対応付けて前記不揮発性メモリの前記破壊読出し領域に退避させるとしてもよい。

[0019] また、本発明の半導体メモリカードにおいて、前記不揮発性メモリは、Ferroelectric Random Access Memory(FeRAM)であるとしてもよい。

[0020] また、本発明のプログラム実行方法は、プログラムを実行可能な半導体メモリカードにおいて前記プログラムを断続的に実行するためのプログラム実行方法であって、前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のプログラムに関する情報を格納するレジスタとを有し、前記プログラム実行方法は、前記半導体メモリカードに対する供給電圧の変化を検出する検出ステップと、前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップとを含む。

[0021] また、本発明の実行プログラムは、アプリケーションプログラムを実行可能な半導体メモリカードにおいて前記アプリケーションプログラムを断続的に実行するための実行プログラムであって、前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のアプリケーションプログラムに関する情報を格納するレジスタとを有し、前記実行プログラムは、前記半導体メモリカードに対する供給電圧の変化を検出する検

出ステップと、前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記アプリケーションプログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップと含む。

[0022] また、本発明の記録媒体は、アプリケーションプログラムを実行可能な半導体メモリカードにおいて前記アプリケーションプログラムを断続的に実行するための実行プログラムが格納された、コンピュータが読み取り可能な記録媒体であって、前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のアプリケーションプログラムに関する情報を格納するレジスタとを有し、前記記録媒体は、前記半導体メモリカードに対する供給電圧の変化を検出する検出ステップと、前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記アプリケーションプログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップとをコンピュータに実行させるための実行プログラムが格納される。

[0023] また、本発明の集積回路は、プログラムを実行可能な半導体メモリカードにおいてプログラムを断続的に実行するための集積回路であって、前記半導体メモリカードは、情報を格納する不揮発性メモリが設けられており、前記集積回路は、実行中のプログラムに関する情報を格納するレジスタと、前記半導体メモリカードに対する供給電圧の変化を検出する検出部と、前記検出部が所定の電圧低下状態を検出した場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避部と、前記検出部が所定の電圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復

帰させる復帰部とを備える。

[0024] 更に、本発明は、本発明の半導体メモリカードの特徴的な構成部をステップとする方法として実現したり、それらのステップを含むプログラムとして実現したり、そのプログラムが格納された、CD－ROM等の記録媒体として実現したり、集積回路として実現することもできる。プログラムは、通信ネットワーク等の伝送媒体を介して流通させることもできる。

発明の効果

[0025] 本発明は、電圧の供給が中断することにより、処理の実行が中断される場合であっても、電圧の供給後に継続して処理を実行することができる半導体メモリカードを提供することができる。

[0026] 本発明によれば、半導体メモリカードにおいて、電圧の供給が不安定な環境などにおいて、処理の実行中に、その処理の実行に必要な電圧の供給が途絶えた場合、処理の実行に必要な電圧の供給が再開されると、中断された処理を継続して実行することができる。つまり、処理を断続的に実行することができる。

[0027] また、2つ以上の独立した処理についても、その処理ごとに断続的に実行することができる。

[0028] また、断続的な処理の実行におけるセキュリティを向上させることができる。つまり、秘匿性の高い情報を扱う処理であっても断続的にかつ安全に実行することができる。

図面の簡単な説明

[0029] [図1]図1は、一般的なICカードのハードウェア構成の一例を示す図

[図2]図2は、実施の形態1のICカードの機能的な構成を示す機能ブロック図

[図3]図3は、実施の形態1のICカードの使用環境および供給電圧の変化を示す概要図

[図4]図4は、実施の形態1における退避情報のデータ構成の一例と、FeRAMのメモリマップの一例を示す図

[図5]図5は、実施の形態1のICカードにおけるレジスタ情報の退避手順を示すフローチャート

[図6]図6は、実施の形態1のICカードにおける処理の再開手順を示すフローチャー

ト

[図7]図7は、実施の形態2のICカードの機能的な構成を示す機能ブロック図

[図8]図8は、非接触型ICカードにおけるTransport Typeの種類を示す図

[図9]図9は、実施の形態2のICカードの使用環境および供給電圧の変化を示す概要図

[図10]図10は、実施の形態2における退避情報のデータ構成の一例と、FeRAMのメモリマップの一例を示す図

[図11]図11は、実施の形態2のICカードにおけるレジスタ情報の退避手順を示すフローチャート

[図12]図12は、実施の形態2のICカードにおいて通信種別を利用してレジスタ情報を復帰させる際の手順を示すフローチャート

[図13]図13は、復帰させるべきレジスタ情報の特定に利用可能な情報の種類を例示する図

[図14]図14は、実施の形態3のICカードの機能的な構成を示す機能ブロック図

[図15]図15は、暗号に関する3種類の情報を示す図

[図16]図16は、CA Typeの種類を示す図

[図17]図17は、実施の形態3における退避情報のデータ構成の一例と、FeRAMのメモリマップの一例を示す図

[図18]図18は、実施の形態3におけるFeRAMの破壊読出し領域および非破壊読出し領域のアドレスを示す図

[図19]図19は、実施の形態3のICカードにおけるレジスタ情報の退避手順を示すフローチャート

[図20]図20は、実施の形態4のICカードの機能的な構成を示す機能ブロック図

[図21]図21は、実施の形態4のICカードにおいてCA Typeを利用してレジスタ情報を復帰させる手順を示すフローチャート

[図22]図22は、実施の形態1のICカードにおける集積回路化の一例を示す図

符号の説明

[0030] 100 ICカード

202 FeRAM

203 アンテナ

300 電圧検出部

301 I／F部

302 退避部

303 復帰部

304 退避判断部

305 認証部

306 復帰判断部

800 通信種別取得部

発明を実施するための最良の形態

[0031] 以下本発明の実施の形態について、図面を参照しながら説明する。

[0032] (実施の形態1)

まず、実施の形態1のICカードの構成を図2を用いて説明する。

図2は、実施の形態1のICカード100の機能的な構成を示す機能ブロック図である。ICカード100は、本発明の半導体メモリカードの一例であり、複数のアプリケーションプログラムを実行可能な非接触型ICカードである。

[0033] ICカード100は、図2に示すように、FeRAM202と、I／F部301と、アンテナ203と、電圧検出部300と、レジスタ205と、退避部302と、復帰部303とを備える。

[0034] なお、ICカード100のハードウェア構成は、図1に示す従来のICカードと同じである。また、以下、レジスタ205に格納されている情報を用いて処理を実行する構成部等、ICカード100が本来有する構成部についての図示および説明は省略し、ICカード100の特徴的な構成部についてのみ図示し説明を行なう。

[0035] FeRAM202は、ICカード100で実行される処理に用いられるデータ等を記憶する不揮発性メモリである。アンテナ203は本発明の半導体メモリカードにおける通信部の一例であり、外部機器との通信I／Fである。ICカード100は、アンテナ203が電波を受信することにより外部機器から電圧の供給を受けることになる。

[0036] 電圧検出部300は、供給電圧の変化を検出する処理部である。レジスタ205は、演

算値や実行状態を保持する記憶素子である。退避部302は、電圧検出部300が所定の電圧低下状態を検出した際、レジスタ205に格納されている実行中のプログラムの演算値や状態についての情報(以下、「レジスタ情報」という。)をFeRAM202に退避させる処理部である。

[0037] 復帰部303は、電圧検出部300が所定の電圧上昇状態を検出した際、FeRAM202に格納されているレジスタ情報がある場合、レジスタ205にそのレジスタ情報を復帰させる処理部である。

[0038] I／F部301は、退避部302および復帰部303とFeRAM202との情報のやり取りを仲介するI／Fである。

[0039] 実施の形態1のICカード100は、上記構成により、必要な電圧の供給を受けられず中断された処理を、電圧供給の再開後に継続して実行することができる。一旦中断された処理を継続して実行する際のICカード100の動作を以下に述べる。

[0040] 図3は、実施の形態1のICカード100の使用環境および供給電圧の変化を示す概要図である。

[0041] 図3に示す使用環境は、各種サービスを提供、管理、保有するサーバ104と、ICカード100と通信を行なう端末装置であるリーダライタ101およびリーダライタ102と、サーバ104とリーダライタ101およびリーダライタ102とを相互に接続するネットワーク103とによって構成される。

[0042] また、ICカード100がリーダライタ101と通信可能なエリアをエリア110とし、リーダライタ102と通信可能なエリアをエリア112とする。エリア110およびエリア112以外のエリアを通信外エリアという。

[0043] サーバ104は、ICカード100にサービスを提供するための少なくとも1個以上のアプリケーションプログラムを有し、そのアプリケーションプログラムを実行する機能を有する。また、リーダライタ101およびリーダライタ102を介し、ICカード100と通信を行なうことによりそのサービスをICカード100に提供する。

[0044] リーダライタ101およびリーダライタ102のそれぞれは、少なくとも、サーバ104から送信される情報をICカード100へ送信する機能と、ICカード100から、サーバ104に対するレスポンス、もしくは、要求を受信し、サーバ104へ送信する機能を有する。

[0045] なお、ICカード100を保有するユーザは、図1の使用環境において等速で移動しており、エリア110、通信外エリア、エリア112の順に通過すると想定する。また、その移動中にICカード100が同一のサービスに対応するための処理をエリア110とエリア112とにおいて継続して行なう場合を想定する。

[0046] 上記移動において、ICカード100は、通信外エリアに入ると電圧の供給が絶たれ、レジスタ205に格納されていた情報は消滅することとなる。そこで、ICカード100では、電圧の供給が完全に絶たれる前に、退避部302がレジスタ情報を不揮発性メモリであるFeRAM202に退避させる。これにより、処理の中断および再開に備えることができる。

[0047] 図4は、実施の形態1における退避情報のデータ構成の一例と、FeRAM202のメモリマップの一例を示す図である。

[0048] 退避情報400は、退避部302によりFeRAM202に退避される情報であり、図4に示すように、フラグ値を示すフラグ情報410と、レジスタ205から収集されたデータ群であるレジスタ情報420とが対応付けられた情報である。

[0049] フラグ値は、“退避データ有り”を示す値または“退避データ無し”を示す値であり、退避部302により設定される。レジスタ情報420がFeRAM202に格納される際は、“退避データ有り”を示す “0xA5A5A5A5”が設定される。

[0050] FeRAM202は、図4に示すように、退避領域401と、記憶領域402と、スタック領域403とを有する。退避情報400が格納される退避領域401は、FeRAM202のアドレス0x0000を先頭アドレスとする所定の領域である。

[0051] 図5は、実施の形態1のICカード100において、電圧検出部300により所定の電圧低下状態が検出され、実行中の処理を中断するためにレジスタ情報420を退避させる手順を示すフローチャートである。

[0052] 図5を用いて、実施の形態1のICカード100がレジスタ情報420を退避させる際の動作を説明する。

[0053] まず、ICカード100がリーダライタ101と通信可能なエリア110に存在する場合、ICカード100は、リーダライタ101を介してサーバ104と通信しサービスの提供を受ける。ICカード100はその通信の開始によりサービスに対応した処理を開始する。

[0054] ICカード100が処理を完了する前に通信外エリアへ移動すると、ICカード100の電圧検出部300は、供給電圧が閾値Vhより低い状態が時間Δtの間継続している状態を検出する。

[0055] 電圧検出部300は上記の電圧低下状態を検出すると、退避部302に電圧低下を知らせるシグナル(以下、「電圧低下シグナル」という。)を発する(S10)。

[0056] 電圧低下シグナルの発生により、レジスタ情報420の退避が開始される。具体的には、まず、退避部302がレジスタ205からレジスタ情報420を収集する(S11)。更に、そのレジスタ情報420に“退避データ有り”を示すフラグ値を付加する(S12)。

[0057] 退避部302は、フラグ値が付加されたレジスタ情報420を、FeRAM202の退避領域へ書き込む(S13)。

[0058] 上記一連の動作により、実行中のプログラムに関するレジスタ情報が不揮発性メモリであるFeRAM202に退避される。これにより、処理の中断に備えることができる。その後、電圧供給量の低下によりレジスタ205に格納されていたレジスタ情報420が消失しても、プログラムの実行に必要な電圧が供給された際には、退避されていたレジスタ情報420をレジスタ205に復帰させることで、処理を再開することができる。

[0059] 図6は、実施の形態1のICカード100において、電圧検出部300により電圧上昇が検出され、処理が再開される手順を示すフローチャートである。

[0060] 図6を用いて、退避されていたレジスタ情報420がレジスタ205に復帰される際のICカード100の動作を説明する。

[0061] 図5に示した一連の動作により、レジスタ情報420が退避領域401に書き込まれた後、ICカード100は通信外エリアからリーダライタ102と通信可能なエリア112へ移動する。ICカード100の電圧検出部300は、エリア112に入ると、供給電圧が閾値Vhより高い状態が時間Δtだけ継続する状態を検出する。

[0062] 電圧検出部300は上記の電圧上昇状態を検出すると、退避部302に電圧上昇を知らせるシグナル(以下、「電圧上昇シグナル」という。)を発する(S20)。

[0063] 電圧上昇シグナルの発生により、レジスタ情報420の復帰が開始される。具体的には、まず、復帰部303は、“退避データ有り”を示すフラグ値が付加されたレジスタ情報420がFeRAM202の退避領域401に格納されているか否かを確認する。

[0064] “退避データ有り”を示すフラグ値が付加されたレジスタ情報420が格納されている場合（S21でYes）、復帰部303は、退避領域401からそのレジスタ情報420を収集する（S22）。更に、収集したレジスタ情報420をレジスタ205へ書き込む（S23）。更に、退避領域401においてレジスタ情報420に付加されている“退避データ有り”を示すフラグ値を消去し、“退避データ無し”の状態に設定する（S24）。また、レジスタ情報420は退避領域401から消去される。

[0065] 上記一連の動作により、電圧の供給が絶たれる前に退避領域401に退避されていたレジスタ情報420が、レジスタ205に復帰される。復帰後、中断されていた処理が再開される。ICカード100は、復帰されたレジスタ情報420の値を用いたプログラムの実行結果をリーダライタ102を介してサーバ104へ送信するなどの通信を行ない、一連の処理を完了する。

[0066] なお、上記動作中、“退避データ有り”を示すフラグ値が付加されたレジスタ情報420が退避領域401に格納されていない場合（S21でNo）は、そのままレジスタ情報の復帰に係る動作は終了する。

[0067] このように、実施の形態1のICカード100は、供給電圧の低下により、実行中の処理が中断される場合であっても、一定レベル以上の電圧の供給が再開されると、中断された処理を中断される前の状態から再開することができる。つまり、処理を断続的に実行することができる。

[0068] なお、本実施の形態では、処理の中断期間を挟み、ICカード100の直接の通信相手が、リーダライタ101からリーダライタ102へ切り換わる場合を想定した。

[0069] しかしながら、処理の中断期間の前後でICカード100の通信相手が同じリーダライタであっても、ICカード100は、レジスタ情報の退避および復帰を行なうことができる。つまり、中断された処理を再開することができる。

[0070] また、レジスタ情報420のレジスタ205への復帰後、レジスタ情報420とレジスタ情報420に付加されたフラグ値とは退避領域401から消去するとしたが、これらは消去しなくてもよい。例えば、レジスタ情報420を用いた処理が正常に完了した後に、フラグ値を、「退避データ無し」に設定し、FeRAM202のいずれかの領域に格納しておいてもよい。こうすることで、例えば、処理の中断前のレジスタ情報420のバックアップ

を確保することができる。

[0071] また、ICカード100が備える不揮発性メモリはFeRAMであるとしたが、FeRAMでなくてもよい。例えば、EEPROMでもよく、電圧の供給が絶たれても、退避された情報を保持しておくことができればよい。

[0072] また、電圧検出部300は、供給電圧が閾値Vhを下回る状態が時間Δtだけ継続した場合、電圧低下シグナルを発し、閾値Vhを上回る状態が時間Δtだけ継続した場合、電圧上昇シグナルを発するとした。しかしながら、上記判断の基準の1つである時間Δtは、電圧低下シグナルを発する場合と、電圧上昇シグナルを発する場合とで同一でなくてもよい。

[0073] また、電圧検出部300は、例えば、供給電圧が閾値Vhを下回った時点で電圧低下シグナルを発してもよく、また、例えば、電圧変化曲線が所定の曲線と近似する場合に、電圧低下シグナルを発してもよい。電圧上昇シグナルを発する場合も同様に、他の判断基準を用いてもよい。更に、これらの判断基準を、実行されるプログラムの種類、ICカード100が使用される環境などに応じて変化させてもよい。

[0074] また、電圧検出部300は供給電圧の変化から所定の電圧低下状態および所定の電圧上昇状態を検出するとした。しかしながら、例えば、電力または電流の変化から所定の状態を検出してもよい。つまり、プログラムの正常な実行に必要な電圧もしくは電流またはその両方の供給の途絶および安定供給の再開を予め検知できれば、電圧以外の物理量の変化を利用してもよい。

[0075] (実施の形態2)

上述の実施の形態1では、ICカード100が、サーバ104から提供される単一のサービスに対応する処理を継続して実行する場合を説明した。実施の形態2では、ICカード100が、複数のサービスのそれぞれに対応する独立した処理を、それぞれの処理ごとに断続的に実行する場合について説明する。

[0076] 図7は、実施の形態2のICカード100の機能的な構成を示す機能ブロック図である。

[0077] 図7に示すように、実施の形態2のICカード100は、外部機器との通信I／Fであるアンテナ203と、供給電圧の変化を検出する電圧検出部300と、電圧検出部300が

発する電圧低下シグナルに基づきレジスタ情報をFeRAM202に退避させる退避部302と、電圧検出部300が発する電圧上昇シグナルに基づき、退避されたレジスタ情報をレジスタ205に復帰させる復帰部303と、退避部302および復帰部303とFeRAM202との情報のやり取りを仲介するI／F部301と、レジスタ情報を記憶する不揮発性メモリであるFeRAM202と、リーダライタとの通信における通信種別を取得する通信種別取得部800とを備える。

[0078] このように、実施の形態2のICカード100は、実施の形態1のICカード100が備える構成部に加え、通信種別取得部800を備えている。

[0079] 通信種別取得部800は、具体的には、リーダライタとの通信により通信プロトコルを示す情報であるTransport Typeを通信種別として取得する。

[0080] 図8は、非接触型ICカードにおけるTransport Typeの種類を示す図である。

[0081] 図8に示すように、非接触型ICカードにおけるTransport Typeには、主にTypeA、TypeB、TypeCとあり、それぞれは、物理レイヤーの仕様の違い、つまり、使用する周波数帯の違いにより判別可能である。

[0082] 本実施の形態では、通信種別取得部800は、取得したTransport Typeをプログラムの種別と対応付けて、退避部302および復帰部303に通知する。退避部302は、通知された情報をレジスタ情報に付加してFeRAM202に退避させる。また、復帰部303は通知された情報を用い、付加された情報が所定の条件を満たすレジスタ情報をFeRAM202の中から選択し復帰させる。

[0083] 実施の形態2のICカード100は、上記構成により、互いに異なる複数の処理のそれぞれを断続的に実行することができる。

[0084] 複数のサービスの提供を受けることができる環境下におけるICカード100の動作を以下に述べる。

[0085] 図9は、実施の形態2のICカード100の使用環境および供給電圧の変化を示す概要図である。

[0086] 図9に示す使用環境は、交通系のサービスを提供するサーバ104と、ネットワーク103を介しサーバ104と相互に接続されるリーダライタ101およびリーダライタ102と、公共系のサービスを提供するサーバ702と、ネットワーク701を介しサーバ702と接

続されるリーダライタ700とによって構成される。

[0087] また、ICカード100がリーダライタ101と通信可能なエリアをエリア110とし、リーダライタ102と通信可能なエリアをエリア112とし、リーダライタ700と通信可能なエリアをエリア703とする。エリア110、エリア112およびエリア703以外のエリアを通信外エリアという。

[0088] サーバ104およびサーバ702のそれぞれは、ICカード100にサービスを提供するための少なくとも1個以上のアプリケーションプログラムを有し、そのアプリケーションプログラムを実行する機能を有する。また、サーバ104はリーダライタ101およびリーダライタ102を介し、サーバ702はリーダライタ700を介し、ICカード100と通信を行なうことにより、それぞれのサービスをICカード100に提供する。

[0089] また、上述のように、サーバ104がICカード100に提供するサービスは交通系のサービスであり、サーバ702がICカード100に提供するサービスは公共系のサービスである。これら公共系のサービスに係る通信の種別と、交通系のサービスに係る通信の種別とは、通信プロトコルにより判別することが可能である。本実施の形態では、公共系のサービスに係る通信の通信プロトコルはTypeBであり、交通系のサービスに係る通信の通信プロトコルはTypeCである。

[0090] リーダライタ101およびリーダライタ102のそれぞれは、少なくとも、サーバ104から送信される情報をICカード100へ送信する機能と、ICカード100から、サーバ104に対するレスポンス、もしくは、要求を受信し、サーバ104へ送信する機能を有する。

[0091] リーダライタ700は、少なくとも、サーバ702から送信される情報をICカード100へ送信する機能と、ICカード100から、サーバ702に対するレスポンス、もしくは、要求を受信し、サーバ702へ送信する機能を有する。

[0092] 実施の形態1の使用環境(図3参照)では、ICカード100を保有するユーザは、サーバ104から提供されるサービスのみを利用可能であったが、図9に示す実施の形態2の使用環境では、上述のように、サーバ104から提供される交通系のサービスに加え、リーダライタ700を介してサーバ702から提供される公共系のサービスを利用することが出来る。

[0093] なお、ICカード100を保有するユーザは、図9の使用環境において等速で移動し

ており、エリア110、通信外エリア、エリア703、通信外エリア、エリア112の順に通過すると想定する。また、その移動中にICカード100がサーバ104から提供される交通系のサービスに対応するための処理を、エリア110とエリア112とにおいて継続して行なう場合を想定する。

[0094] 上記移動において、ICカード100は、エリア110から通信外エリアに入ると電圧の供給が絶たれ、レジスタ205に格納されていた情報は消滅することとなる。そこで、ICカード100では、電圧の供給が完全に絶たれる前に、退避部302がレジスタ情報と通信種別に基づく情報とを対応付けて不揮発性メモリであるFeRAM202に退避させる。これにより、サーバ104との通信を再開することのできるエリア112に入った後に処理を再開することができる。

[0095] なお、ICカード100は、エリア112に到達する前に、サーバ702と通信することのできるエリア703を通過するが、エリア703に入った際、サーバ702との通信に対応するプログラムの実行が中断されていないか判断される。この判断は、通信種別に基づいて行なわれる。本実施の形態では、サーバ104との通信に関係するレジスタ情報のみが退避されており、そのレジスタ情報は復帰されない。また、サーバ702から提供される公共系のサービスに対応したプログラムが起動され、そのプログラムによる処理が開始される。

[0096] 上記処理を完了する前に、ICカード100がエリア703から通信外エリアへ移動すると、エリア110から通信外エリアへ移動する場合と同じく、処理が中断され、レジスタ情報がFeRAM202に退避される。このとき、中断する直前のレジスタ情報は、エリア110から通信外エリアへ移動する際にレジスタ情報が格納された領域とは異なる領域へ格納される。

[0097] 図10は、実施の形態2における退避情報のデータ構成の一例と、FeRAM202のメモリマップの一例を示す図である。

[0098] 退避情報900は、退避部302によりFeRAM202に退避される情報であり、図10に示すように、フラグ値とType Informationとを含む識別情報910と、レジスタ205から収集されたデータ群であるレジスタ情報420とが対応付けられた情報である。

[0099] フラグ値は、実施の形態1と同じく“退避データ有り”を示す値または“退避データ無

し”を示す値であり、退避部302により設定される。レジスタ情報420がFeRAM202に格納される際は、“退避データ有り”を示す“0xA5A5A5A5”が設定される。

[0100] Type Informationは、本発明の半導体メモリカードにおける付加情報の一例であり、レジスタ情報420を用いた処理を行なうプログラムを特定するための情報である。本実施の形態では、Type Informationとして通信種別に基づく情報が設定される。

[0101] 具体的には、通信種別取得部800がリーダライタとの通信により、“TypeB”を取得した場合は、公共アプリケーションプログラム(公共AP)と対応付けられ、“公共AP(TypeB)”を示す値が設定される。“TypeC”を取得した場合は、同様に“交通AP(TypeC)”を示す値が設定される。

[0102] FeRAM202は、図10に示すように、第1退避領域901と、第2退避領域902と、記憶領域402と、スタック領域403とを有する。第1退避領域901は、FeRAMのアドレス0x0000を先頭アドレスとする所定の領域であり、第2退避領域901は、FeRAMのアドレス0x003Cを先頭アドレスとする所定の領域である。

[0103] 図11は、実施の形態2のICカード100において、電圧検出部300により所定の電圧低下状態が検出され、実行中の処理を中断するためにレジスタ情報420を退避させる手順を示すフローチャートである。

[0104] 図11を用いて、実施の形態2のICカード100がレジスタ情報420を退避させる際の動作を説明する。

[0105] まず、ICカード100がリーダライタ101と通信可能なエリア110に存在する場合、ICカード100は、リーダライタ101を介してサーバ104と通信し交通系のサービスの提供を受ける。ICカード100はその通信の開始により交通系のサービスに対応した処理を開始する。

[0106] ICカード100が処理を完了する前に通信外エリアへ移動すると、ICカード100の電圧検出部300は、供給電圧が閾値Vhより低い状態が時間Δtの間継続している状態を検出する。

[0107] 電圧検出部300は上記の電圧低下状態を検出すると、退避部302に電圧低下を知らせるシグナルを発する(S10)。

[0108] 電圧低下シグナルの発生により、レジスタ情報420の退避が開始される。具体的には、まず、退避部302がレジスタ205からレジスタ情報420を収集する(S11)。

[0109] 退避部302は、更に、“退避データ有り”を示すフラグ値と、通信種別取得部800から通知された通信種別に基づく情報とをレジスタ情報420に付加する(S32)。具体的には、退避データ有り”を示すフラグ値と“交通AP(TypeC)”を含む識別情報910がレジスタ情報420に付加される。

[0110] 退避部302は、識別情報910が付加されたレジスタ情報420を、第1退避領域901へ退避可能か否かを調べる。退避可能な場合(S33でYes)、識別情報910が付加されたレジスタ情報420を第1退避領域901へ退避させる。第1退避領域901に別のレジスタ情報が格納されているなど、退避不可能な場合(S33でNo)は、第2退避領域902へ退避させる。

[0111] 上記一連の動作により、交通系のサービスに対応して動作中であったプログラムに関するレジスタ情報420が、そのプログラムを特定するための情報とともに不揮発性メモリであるFeRAM202に退避される。

[0112] この後、通信外エリアからエリア703に入ると、電圧検出部300により所定の電圧上昇状態を検出される。更に、起動されるプログラムに対応するレジスタ情報、つまり、復帰させるべきレジスタ情報がFeRAM202に格納されている場合、復帰部303によりそのレジスタ情報がレジスタ205に復帰される。

[0113] 図12は、実施の形態2のICカード100において、通信種別を利用してレジスタ情報を復帰させる際の手順を示すフローチャートである。

[0114] 図12を用いて、通信種別に基づく判断の下にレジスタ情報420を復帰させる際のICカード100の動作を説明する。図11を用いて説明した一連の動作により、レジスタ情報420が退避領域901に書き込まれている場合を想定し、以下の説明を行なう。

[0115] ICカード100は通信外エリアからリーダライタ700と通信可能なエリア703へ移動する。ICカード100の電圧検出部300は、エリア703に入ると、供給電圧が閾値Vhより高い状態が時間Δtだけ継続する状態を検出する。

[0116] 電圧検出部300は上記の電圧上昇状態を検出すると、退避部302に電圧上昇を知らせるシグナルを発する(S20)。

[0117] 電圧上昇シグナルの発生により、レジスタ情報420の復帰が開始される。具体的には、まず、通信種別取得部800により、リーダライタ700との通信における通信種別が取得される(S41)。

[0118] リーダライタ700は、公共系のサービスを提供するサーバ702とICカード100との通信を中継する端末であり、通信プロトコルはTypeBである。従って、通信種別取得部800により“TypeB”が取得される。通信種別取得部800はTypeBと、対応するプログラム種別である“公共AP”とを対応付け“公共AP(TypeB)”を示す情報を復帰部303に通知する。

[0119] 復帰部303は、“公共AP(TypeB)”が付加されたレジスタ情報が第1退避領域901または第2退避領域902に格納されているか否かを調べる。

[0120] 本実施の形態においては、第1退避領域901に格納されているレジスタ情報420は、“交通AP(TypeC)”が付加されたものである。従って、復帰させるべきレジスタ情報は存在しないと判断する(S42でNo)。復帰させるべきレジスタ情報がないと判断すると、レジスタ情報の復帰に係る動作は終了する。

[0121] その後、サーバ702から提供される公共系のサービスに対応するプログラムが起動され、処理が開始される。その処理の完了前に、エリア703から通信外エリアへ移動すると、処理が中断され、レジスタ情報がFeRAM202に退避される。このとき、FeRAM202の第1退避領域901には、サーバ104との通信に対応するレジスタ情報420が格納されている。そのため、サーバ702との通信に対応するレジスタ情報は第2退避領域902へ退避される。

[0122] このように、第1退避領域901にサーバ104との通信に対応するレジスタ情報420が格納され、第2退避領域902にサーバ702との通信に対応するレジスタ情報が格納されている状態で、ICカード100がエリア112に移動した際の動作を、図12を用いて説明する。

[0123] ICカード100の電圧検出部300により所定の電圧上昇状態が検出され、電圧上昇シグナルが発せられる(S20)。これにより以下に示すレジスタ情報420の復帰処理が開始される。

[0124] 通信種別取得部800は、リーダライタ102との通信における通信種別を取得する。

リーダライタ102は、交通系のサービスを提供するサーバ104とICカード100との通信を中継する端末であり、通信プロトコルはTypeCである。従って、通信種別取得部800により“TypeC”が取得される。通信種別取得部800はTypeCと対応するプログラム種別と対応付け“交通AP[TypeC]”を示す情報を復帰部303に通知する。

[0125] 復帰部303は、“交通AP[TypeC]”が付加されたレジスタ情報420が第1退避領域901または第2退避領域902に格納されているか否かを調べる。

[0126] 本実施の形態では、第1退避領域901に“交通AP[TypeC]”が付加されたレジスタ情報420、つまり復帰させるべきレジスタ情報が存在し(S42でYes)、復帰部303は、第1退避領域901からそのレジスタ情報420を収集する(S43)。更に、収集したレジスタ情報420をレジスタ205へ書き込む(S44)。

[0127] なお、復帰させるべきレジスタ情報が存在しない場合(S42でNo)、レジスタ情報に係る動作を終了する。

[0128] 上記一連の動作により、ICカード100は、エリア110から外れることで中断されていた交通系のサービスに対応する処理を再開することができる。ICカード100は、復帰されたレジスタ情報420を用いたプログラムの実行結果をリーダライタ102を介してサーバ104へ送信するなどの通信を行ない、一連の処理を完了する。

[0129] なお、第2退避領域902に格納されているレジスタ情報は、ICカード100が、エリア703のようにサーバ702と通信可能なエリアへ移動すると、レジスタ205に復帰される。更に、このレジスタ情報が用いられ、公共系のサービスに対応した処理が再開されることとなる。この処理の再開の際のICカード100の動作は、上述の交通系のサービスに対応する処理の再開の際の動作と同様である。

[0130] このように、実施の形態2のICカード100は、実施の形態1のICカード100と同じく、中断された処理を中断時の状態から再開することができる。つまり、処理を継続して行なうことができる。また、実施の形態2のICカード100では、2つの独立したレジスタ情報を別々に格納することができ、それぞれのレジスタ情報には通信種別に基づく情報が付加される。

[0131] これにより、電圧の供給が再開した際に、起動されるプログラムに対応するレジスタ情報を正しく選択し、復帰させることができる。また、FeRAM202に退避されている

レジスタ情報が、起動されるプログラムに対応しないものである場合、そのレジスタ情報は格納されたままにされる。これにより、中断された処理を中断された時点の状態で維持することができる。また、2つの独立した処理のそれぞれをこのように中断された時点の状態で維持することができる。これにより、それぞれの処理を断続的に実行することができる。

[0132] なお、本実施の形態では、サーバ104およびサーバ702から提供される交通系のサービスおよび公共系のサービスに対応するそれぞれの処理をICカード100が断続的に実行する場合を説明した。

[0133] しかしながら、ICカード100が処理する内容は、交通系等のサービスの種別に限定されることはなく、また、3つ以上の独立した処理を行なわせてもよい。

[0134] この場合、ICカード100は、それら処理に対応する実行可能なプログラムを有しておき、FeRAM202は必要なだけ退避領域を有しておけばよい。これにより、より多くの数の独立した処理のそれぞれを断続的に実行することができる。

[0135] また、通信種別取得部800は、取得した通信種別とプログラムの種別とを対応付けて退避部302および復帰部303に通知するとした。しかしながら、通信種別のみを通知してもよい。つまり、再開される処理、具体的には起動されるプログラムを特定できるのであれば通信種別のみでもよい。

[0136] また、通信種別取得部800は、電力供給を受けた際に判別可能な通信種別を先行して通知し、その後、必要に応じてプログラムの種別を通知するとしてもよい。この場合、例えば、新たに開始された通信の通信種別が“TypeB”であり、かつ、退避されているレジスタ情報420が“TypeC”と対応付けられたものであれば、レジスタ情報420の復帰処理が不要であると判定できる。つまり、プログラム種別が何であるかの解析等を行なう必要がない場合が存在し、レジスタ情報の復帰に係る処理の速度を向上させることができる。

[0137] また、通信種別以外の情報を利用し、復帰させるべきレジスタ情報の存在の確認および選択を行なってもよい。つまり、ICカード100において実行が中断され再開されるプログラムを特定できる情報であれば通信種別以外の情報を利用してもよい。

[0138] 図13は、復帰させるべきレジスタ情報の特定に利用可能な情報の種類を例示する

図である。図13に示す各種の情報のそれぞれ、または、それぞれの組み合わせからなる情報は、本発明の半導体メモリカードにおける付加情報の一例である。

[0139] 図13に示すように、復帰させるべきレジスタ情報の特定に利用する情報は、通信種別である通信プロトコルを示すTransport Type以外の情報でもよい。

[0140] 例えば、通信プロトコルそのものでなく、通信プロトコルを特定できる情報である通信プロトコル長を示すTransport info lengthや、通信プロトコルに関する情報を示すTransport Informationを利用してもよい。

[0141] また、アプリケーションプログラムの識別子を示すApplication ID、アプリケーションプログラムの種別を示すApplication Typeや、中断と再開とを複数回繰り返す処理をバージョン管理するための情報であるResume Versionを利用してもよい。

[0142] 本実施の形態のICカード100は、通信種別を取得するために通信種別取得部800を備えているが、上述の、通信種別以外の情報を取得して利用する場合、通信種別取得部800に換えて、または、通信種別取得部800に加えて、他の情報を取得するための取得部を備えればよい。

[0143] 例えば、Application IDを利用する場合、リーダライタとの通信、または、実行中のプログラム自身からApplication IDを取得するID取得部を備えればよい。

[0144] 退避部302は、電圧検出部300から電圧低下シグナルを受け取ると、ID取得部により取得された、実行中のプログラムを特定する情報であるApplication IDをレジスタ情報に付加してFeRAM202に退避させる。その後、復帰部303は、電圧検出部300から電圧上昇シグナルを受け取るとともに、リーダライタとの通信内容からID取得部が取得したApplication IDを受け取る。復帰部303は、受け取ったApplication IDが付加されたレジスタ情報をFeRAM202の中から読出し、レジスタ205に復帰させる。

[0145] 復帰されたレジスタ情報は、起動するプログラムに対応するものであり、中断されていた処理が、そのレジスタ情報を用いて再開される。

[0146] このように、通信種別以外の情報を利用した場合であっても、中断した処理を再開させることができる。つまり、処理を断続的に実行することができる。

[0147] また、図13に示す複数の種類の情報それぞれをレジスタ情報に直接付加するので

はなく、対応付けられた別の情報を付加させてもよい。例えば、Application IDを直接レジスタ情報に付加するのではなく、Application IDに対応するプログラム名を付加してもよい。この場合、その対応付けをFeRAM202の所定の領域に格納しておけばよい。つまり、ICカード100がリーダライタとの通信により得られた情報が、レジスタ情報420に付加された情報に実質的に含まれているか否かの判断ができればよい。

[0148] また、複数の種類の情報を組み合わせてレジスタ情報420に付加させてもよい。この場合、ICカード100は、リーダライタとの通信内容からその複数の種類の情報を取得し、更に、取得した複数の種類の情報の全てが付加されたレジスタ情報420を復帰させるとしてもよい。これにより、例えば、復帰させるべきレジスタ情報420の特定をより厳密に行なうことができる。

[0149] (実施の形態3)

実施の形態3として、実施の形態1および2のICカード100のセキュリティを向上させるための構成について説明を行なう。ICカード100のセキュリティを向上させることにより、秘匿性の高い情報の処理を断続的に、かつ、より安全に実行することができる。なお、具体的な説明および図示は実施の形態2のICカード100を基礎として行なう。また、実施の形態3のICカード100の使用環境は、実施の形態1または実施の形態2と同じである。

[0150] 図14は、実施の形態3のICカード100の機能的な構成を示す機能ブロック図である。

[0151] 図14に示すように、実施の形態3のICカード100は、外部機器との通信I／Fであるアンテナ203と、供給電圧の変化を検出する電圧検出部300と、電圧検出部300が発する電圧低下シグナルに基づきレジスタ情報をFeRAM202に退避させる退避部302と、電圧検出部300が発する電圧上昇シグナルに基づき、退避されたレジスタ情報をレジスタ205に復帰させる復帰部303と、退避部302および復帰部303とFeRAM202との情報のやり取りを仲介するI／F部301と、レジスタ情報を記憶する不揮発性メモリであるFeRAM202と、リーダライタとの通信における通信種別を取得する通信種別取得部800とを備える。

[0152] FeRAM202は、破壊読出し領域と非破壊読出し領域とで構成されている。破壊読出し領域とは、データが読み出された後に読み出されたデータの補充が行なわれず、データが残らない領域のことである。FeRAM202の構成については、図17を用いて後述する。

[0153] また、退避部302は、退避判断部304を有する。退避判断部304は、実行が中断されるプログラムが利用する暗号の暗号化強度に基づき、レジスタ情報を破壊読出し領域と非破壊読出し領域とのどちらに退避させるかを判断する処理部である。

[0154] このように、実施の形態3のICカード100は、特徴的な構成部として、実施の形態2のICカード100が備える構成部に加え退避判断部304を備えている。

[0155] 退避判断部304は、実行が中断されるプログラムが利用する暗号の暗号化強度が所定の強度以上であれば、FeRAM202の破壊読出し領域に退避させる。

[0156] 暗号化強度が所定の強度以上であるということは、そのプログラムが扱うデータの秘匿性が高いと考えられる。そのため、レジスタ情報を破壊読出し領域に退避させる。これにより、秘匿性が高いと考えられるレジスタ情報がICカード100外に読み出される危険性を低くすることができる。つまりICカード100のセキュリティを向上させることができる。

[0157] 暗号化強度を特定するための情報として本実施の形態では、暗号化方式を示す情報であるConditional Access(CA) Typeを利用する。

[0158] 図15は、暗号に関する3種類の情報を示す図である。CA Typeは、本発明の半導体メモリカードにおける暗号情報の一例であり、暗号化強度を示す情報である。具体的には、CA Typeにより、暗号化方式を示すCA種別が特定され、CA種別により暗号化強度が特定される。CA Key lengthは、暗号化に用いる鍵の長さを示す情報であり、CA Keyは、鍵そのものを示す情報である。

[0159] 図16は、CA Typeの種類を示す図である。代表的なCA Typeとして、Single Data Encryption Standard(Single DES)方式を示すM__CA__DESと、Triple DES(3DES)方式を示すM__CA__3DESと、RSA方式を示すM__CA__RSAとがある。これら暗号化方式は、Single DES、3DES、RSAの順に暗号化強度が強くなる。なお、NO__USEは暗号化なし、つまり、処理を実行するプログラムが暗

号を利用してないことを示すCA Typeである。

[0160] これらCA Typeには、それぞれ図に示す値が割り当てられており、ICカード100において実行されるプログラムはこの値を有している。図14に示すICカード100の退避判断部304は、レジスタ情報を退避させる際に、実行が中断されるプログラムからこの値を読出し、そのプログラムが利用する暗号化方式を特定する。更に、本実施の形態では、暗号化強度が、3DESの暗号化強度より高い場合、レジスタ情報をFeRAM202の破壊読出し領域に退避させる。

[0161] つまり、実行が中断されるプログラムが利用する暗号化方式が、3DESまたはRSAであれば、退避部302は、退避判断部304の判断により、レジスタ情報をFeRAM202の破壊読出し領域に退避させることとなる。

[0162] 図17は、実施の形態3における退避情報のデータ構成の一例と、FeRAM202のメモリマップの一例を示す図である。

[0163] 退避情報950は、退避部302によりFeRAM202に退避される情報であり、図17に示すように、フラグ値とType InformationとCA Typeとを含む識別情報920と、レジスタ205から収集されたデータ群であるレジスタ情報420とが対応付けられた情報である。

[0164] フラグ値は、実施の形態1および2と同じく“退避データ有り”を示す値または“退避データ無し”を示す値であり、FeRAM202に退避される際には“退避データ有り”を示す値に設定される。

[0165] Type Informationは、レジスタ情報420を用いた処理を行なうプログラムを特定するための情報であり、実施の形態2と同じく通信種別に基づく情報である。

[0166] CA Typeは、上述のように実行が中断されたプログラムが利用する暗号化方式を示す情報である。暗号化なし、Single DES、3DES、RSAのいずれかを示す値が退避判断部304によりプログラムから読み出され、レジスタ情報420にCA Typeとして付加される。

[0167] FeRAM202は、図17に示すように、破壊読出し領域202aと非破壊読み出し領域202bとから構成される。破壊読出し領域202aは第1退避領域911を有し、非破壊読み出し領域202bは、第2退避領域912と、記憶領域402と、スタック領域403とを

有する。

[0168] 図18は、本実施の形態におけるFeRAM202の破壊読出し領域202aおよび非破壊読出し領域202bのアドレスを示す図である。破壊読出し領域202aおよび非破壊読出し領域202bのそれぞれは、図18に示すように、FeRAM202のメモリ空間の連続するアドレスに存在する。

[0169] 上述のように、レジスタ情報420に付加されたCA Typeが3DESまたはRSAを示す値であれば、レジスタ情報420は、破壊読出し領域202aに存在する第1退避領域911に退避される。また、CA Typeが3DESまたはRSA以外を示す値であれば、非破壊読出し領域202bに存在する第2退避領域912に退避される。

[0170] 図19は、実施の形態3のICカード100において、電圧検出部300により所定の電圧低下状態が検出され、実行中の処理を中断するためにレジスタ情報420を退避させる手順を示すフローチャートである。

[0171] 図19を用いて、実施の形態3のICカード100がレジスタ情報420を退避させる際の動作を説明する。

[0172] 上述の実施の形態1および2と同様に、電圧検出部300が所定の電圧低下状態を検出し、電圧低下シグナルを発する(S10)。これによりレジスタ情報の退避が開始され、退避部302によりレジスタ205からレジスタ情報420が収集される(S11)。

[0173] 退避判断部304は、実行を中断されるプログラムからCA Typeを読み出す。退避部302は、レジスタ情報420に“退避データ有り”を示すフラグ値と、通信種別取得部800により取得された通信種別と、暗号化方式を示すCA Typeとを付加する(S52)。

[0174] 退避判断部304は、読み出したCA Typeによって特定される暗号化方式の暗号化強度が所定の強度以上であるか否かにより、レジスタ情報420を退避させる領域を判断する。

[0175] 具体的には、暗号化方式が3DESまたはRSAである場合(S53でYes)、レジスタ情報420をFeRAM202の破壊読出し領域202aにある第1退避領域911に退避させると判断する。退避部302は、この判断に従い、フラグ値等が付加されたレジスタ情報420を第1退避領域911に退避させる(S54)。

[0176] また、3DESもしくはRSA以外の暗号化方式である場合、または、暗号化なしである場合(S53でNo)、レジスタ情報420をFeRAM202の非破壊読出し領域202bにある第2退避領域912に退避させると判断する。退避部302は、この判断に従い、フラグ値等が付加されたレジスタ情報420を第2退避領域912(S55)に退避させる。

[0177] 上記一連の動作により、実行中のプログラムに関するレジスタ情報が、不揮発性メモリであるFeRAM202に退避される。

[0178] ICカード100は、実施の形態1および2の説明で述べたように、複数の処理のそれぞれを断続的に実行することが可能であり、FeRAM202は複数のレジスタ情報を格納しておくことができる。本実施の形態では、更に、レジスタ情報の退避前に、プログラムの暗号化強度を特定し、暗号化強度が高く、重要性が高いと考えられるレジスタ情報を優先的に破壊読出し領域に退避させることができる。

[0179] 一般にICカードがリーダライタと通信を開始する際、ICカードとリーダライタとの間で暗号化処理を伴う認証処理が行なわれる。また、その暗号化処理についての情報を含む認証処理の情報もレジスタ情報に含まれる。そのため、レジスタ情報を破壊読出し領域202aに退避させることはICカード100のセキュリティ向上の観点から有益である。

[0180] なお、本実施の形態において、レジスタ情報420を退避させる際、CA Typeを付加するとしたが、CA Typeを付加させなくてもよい。レジスタ情報420を退避させる前に、退避判断部304がCA Typeに基づき退避させる領域を判断できればよく、この判断後に破棄してもよい。

[0181] また、レジスタ情報420に付加され退避されたCA Typeを、レジスタ情報420を復帰させる際に利用してもよい。例えば、レジスタ情報を復帰させる際、付加されているCA Typeを確認し、3DESより高い暗号化強度を有する暗号化方式である場合、リーダライタの認証を行なってからレジスタ情報を復帰させてもよい。

[0182] レジスタ情報420を復帰させる際にCA Typeを利用するための構成については実施の形態4として後述する。

[0183] また、CA Typeによって特定される暗号化強度が所定の強度以上である場合、レジスタ情報をFeRAM202の破壊読出し領域202aにある第1退避領域911に退避さ

せるとした。

[0184] しかしながら、例えば、第1退避領域911が十分に大きい場合など、レジスタ情報を常に第1退避領域911に退避させてもよい。または、通常は第1退避領域911にレジスタ情報を退避させ、第1退避領域911の残量が所定の容量以下になった場合にのみ、上述のCA Typeに基づく判断を行ない、秘匿性が高いと認められるレジスタ情報のみを第1退避領域911に退避させるとしてもよい。このように、ICカード100のリソースに応じてセキュリティの向上を図ることができる。

[0185] また、退避させる退避領域の判断にCA Typeを使用したが、Ca Type以外の情報を利用してもよい。例えば、図15に示すCA Key lengthでもよい。CA Key lengthは鍵長を示す情報であり、鍵長が長いほど暗号化強度が高いといえる。そこで、CA Key lengthが所定の長さ以上の鍵長を示す場合、対応するレジスタ情報を破壊読出し領域202aに退避させるとしてもよい。さらに、これらの情報を複合させて、レジスタ情報を破壊読出し領域202aに退避させるか否かの判断を行なってもよい。

[0186] また、CA TypeがDESまたはRSAの場合、レジスタ情報を破壊読出し領域202aに退避させるとしたが、別の判断基準でもよい。例えば、CA TypeがRSAの場合のみ、レジスタ情報を破壊読出し領域202aに退避させるとしてもよい。また、例えば、DESより暗号化強度の高い暗号化方式を示すCA Typeであれば、レジスタ情報を破壊読出し領域202aに退避させるとしてもよい。

[0187] また、退避判断部304が、CA Typeにより特定される暗号化強度が所定の強度以上であるかを判断するのは、レジスタ情報にフラグ値等が付加された後でなくてもよい。例えば、電圧検出部300により電圧低下シグナルが発せられる前でもよい。この場合、その判断結果を所定の記憶領域に記憶させておけばよい。レジスタ情報を退避させる前に、その判断結果を用い、レジスタ情報を破壊読出し領域202aに退避させるか否かの判断が可能であればよい。

[0188] このように、ICカード100のユーザの利用形態や、実行されるプログラムの種類等に応じ、レジスタ情報を破壊読出し領域202aに退避させるか否かの判断に利用する情報の種別および判断基準を変更してもよい。また、処理手順も上述の実施の形態

で説明した手順以外でもよい。こうすることで、例えば、ICカード100が扱う情報の秘匿性に応じたセキュリティ対策を施すことができる。また、これら変更により、処理を断続的に実行できるというICカード100の特徴は失われるものではない。

[0189] （実施の形態4）

実施の形態3では、レジスタ情報を退避させる際に暗号化強度を示す情報を利用し、実施の形態1および2のICカード100のセキュリティを向上させる構成について説明した。

[0190] 実施の形態4では、レジスタを復帰させる際に暗号化強度を示す情報を利用し、ICカード100のセキュリティを向上させる構成について説明する。

[0191] つまり、実施の形態4のICカード100においても実施の形態3と同様に、秘匿性の高い情報の処理を断続的に、かつ、より安全に実行することができる。

[0192] なお、具体的な説明および図示は実施の形態2のICカード100を基礎として行なう。また、実施の形態4のICカード100の使用環境は、実施の形態1または実施の形態2と同じである。

[0193] 図20は、実施の形態4のICカード100の機能的な構成を示す機能ブロック図である。

[0194] なお、FeRAM202には、図17に示した、CA Typeが付加されたレジスタ情報420が格納されると想定する。CA Typeは、退避部302により、実行を中断されるプログラムから取得され、レジスタ情報に付加される。

[0195] 図20に示すように、実施の形態4のICカード100は、外部機器との通信I／Fであるアンテナ203と、供給電圧の変化を検出する電圧検出部300と、電圧検出部300が発する電圧低下シグナルに基づきレジスタ情報をFeRAM202に退避させる退避部302と、電圧検出部300が発する電圧上昇シグナルに基づき、退避されたレジスタ情報をレジスタ205に復帰させる復帰部303と、退避部302および復帰部303とFeRAM202との情報のやり取りを仲介するI／F部301と、レジスタ情報を記憶する不揮発性メモリであるFeRAM202と、リーダライタとの通信における通信種別を取得する通信種別取得部800とを備える。

[0196] また、復帰部303は、認証部305と復帰判断部306とを有する。復帰判断部306は

、レジスタ情報に付加されFeRAM202に退避されたCA Typeに基づき、認証処理を行なうか否かを判断する処理部である。認証部305は、復帰判断部306の判断に従い、リーダライタとの間で認証処理を実行する処理部である。

[0197] このように、実施の形態4のICカード100は、特徴的な構成部として、実施の形態2のICカード100が備える構成部に加え、認証部305と復帰判断部306とを備えている。

[0198] 復帰判断部306は、復帰対象のレジスタ情報に付加されたCA Typeから暗号化強度を特定する。特定した暗号化強度が所定の強度以上であれば、認証部305がリーダライタの認証を行なう。復帰部303は、認証部305による認証が成功した場合のみ、そのレジスタ情報を復帰させる。

[0199] 具体的には、本実施の形態においては、CA Typeが示す暗号化方式が3DESまたはRSAである場合、リーダライタの認証を行なう。

[0200] なお、一般に、ICカードとリーダライタとは、通信を開始する際、相互を認証するための処理を実効する。ICカード100においても、リーダライタとの通信の開始の際に、認証処理が実行される。さらに、処理の中断前に、認証処理に関する情報もレジスタ情報に含められ退避される。そのため、再度の認証処理を行なわずに、退避されたレジスタ情報に含まれる認証処理に関する情報を利用し、中断していた処理を再開することは可能である。

[0201] しかしながら、実施の形態4のICカード100は、レジスタ情報に付加されているCA Typeが所定の強度以上の暗号化方式を示す場合、リーダライタに対する認証処理を実行する。認証が成功した場合、つまり、リーダライタの正当性を確認することができた場合のみレジスタを復帰させる。これにより、ICカード100のセキュリティを向上させることができる。

[0202] なお、リーダライタとの間の認証処理を実行する構成部はICカードに本来備えられており、図示および説明は省略したが実施の形態1～3のICカード100においても備えられている。

[0203] 図21は、実施の形態4のICカード100において、CA Typeを利用してレジスタ情報を復帰させる手順を示すフローチャートである。

[0204] 図21を用いて、CA Typeに基づく判断の下にレジスタ情報420を復帰させる際のICカード100の動作を説明する。

[0205] 上述の実施の形態1および2と同様に、電圧検出部300が所定の電圧上昇状態を検出し、電圧上昇シグナルを発する(S20)。これによりレジスタ情報の復帰が開始され、まず、通信種別取得部800により、リーダライタ700との通信における通信種別が取得される(S41)。復帰部303は、フラグ値が"退避データ有り"を示す値であり、かつ、取得された通信種別に対応するレジスタ情報420がFeRAM202に格納されているか否かを調べる。

[0206] 上記条件に該当するレジスタ情報420が格納されている場合(S42でYes)、復帰判断部306は、そのレジスタ情報420に付加されているCA Typeを参照し、CA Typeが3DESまたはRSAを示す値であるか否かを確認する。3DESまたはRSAを示す値である場合(S63でYes)、認証処理の実行を認証部305に指示する。

[0207] 認証部305は、リーダライタの認証を行なう(S64)。認証が成功すると(S65でYes)、復帰部303は、FeRAM202からレジスタ情報420を収集し(S66)、レジスタ205へ書き込む(S67)。

[0208] 上記一連の動作により、レジスタ情報420はレジスタ205へ復帰され、処理が再開される。

[0209] なお、復帰させるべきレジスタ情報420がFeRAM202に格納されていない場合(S42でNo)、および、認証部305による認証が成功しなかった場合(S65でNo)は、レジスタ情報の復帰は行なわれることなく、レジスタ情報の復帰に係る動作は終了する。

[0210] また、復帰させるべきレジスタ情報420がFeRAM202に格納されている(S42でYes)が、そのレジスタ情報に付加されたCA Typeが3DESまたはRSAを示す値でない場合は、認証は行われず、レジスタ情報420の収集(S66)へ進む。CA Typeがレジスタ情報420に付加されていない場合も同じである。

[0211] このように、実施の形態4のICカード100は、中断された処理を再開する際、つまり退避されているレジスタ情報を復帰させる際、そのレジスタ情報に付加されたCA Typeから暗号化強度を特定する。特定した暗号化強度が所定の強度以上である場合

、リーダライタの認証を行なう。認証が成功すると、つまり、直接の通信相手であるリーダライタの正当性を確認することができると、レジスタ情報を復帰させる。

[0212] 例えばCA TypeがRSAを示す値である場合、そのCA Typeが付加されたレジスタ情報は、秘匿性の高い情報であると考えられる。そこで、ICカード100は、通信相手のリーダライタの正当性を確認した上で、レジスタ情報を復帰させ処理を再開する。これにより、不正にレジスタ情報が読み出される、または利用されることを防ぐことができる。つまり、ICカード100のセキュリティを向上させることができる。

[0213] なお、本実施の形態において、処理の再開前にリーダライタの認証を行なうか否かの判断にCA Typeを利用したが、CA Type以外の情報を利用してもよい。例えば、図15に示すCA Key lengthを利用してもよい。実施の形態3の説明で述べたように、CA Key lengthは鍵長を示す情報であり、鍵長が長いほど暗号化強度が高いといえる。そこで、復帰させるべきレジスタ情報に付加されたCA Key lengthが所定の長さ以上の鍵長を示す場合、上記認証処理を行なってもよい。更に、これらの情報を複合させてレジスタ情報に付加して退避させておき、複合された情報により、上記認証処理を行なうか否かを判断してもよい。

[0214] また、CA TypeがDESまたはRSAの場合、リーダライタの認証を行なうとしたが、別の基準で判断してもよい。例えば、CA TypeがRSAの場合のみ、認証処理を行なうとしてもよく、また、例えば、DESより暗号化強度の高い暗号化方式を示すCA Typeであれば、認証処理を行なうとしてもよい。

[0215] また、CA Typeが何であるかに関わらず、処理の再開前には常にリーダライタの認証を行なうとしてもよい。

[0216] このように、処理の再開前の認証処理を行なうか否かの判断に利用する情報の種別、および判断基準は、本実施の形態で用いたもの以外でよい。こうすることで、例えば、ICカード100が扱う情報の秘匿性に応じたセキュリティ対策を施すことができる。また、これら変更により、処理を断続的に実行できるというICカード100の特徴は失われるものではない。

[0217] また、本実施の形態のICカード100の特徴に、実施の形態3のICカード100の特徴を加えてもよい。具体的には、図20に示す本実施の形態のICカード100の構成に

、図14に示す実施の形態3のICカード100が有する退避判断部304を加えてもよい。

[0218] この場合、FeRAM202は、図17に示すように破壊読出し領域202aを有し、その中にレジスタ情報を退避する領域を有していればよい。

[0219] こうすることで、ICカード100では、処理の再開前に通信相手の正当性の確認が行なわれ、処理の再開後には、その処理に用いられるレジスタ情報はFeRAM202に残らないことになる。これにより、秘匿性の高いと考えられるレジスタ情報をより強固に保護することができ、ICカードのセキュリティを更に向上させることができる。

[0220] (実施の形態1～4の第1の補足事項)

以上、実施の形態1～4について説明した。なお、これまでの説明においてICカード100が備える、電圧検出部300、退避部302、I／F部301、復帰部303、通信種別取得部800、退避判断部304、認証部305および復帰判断部306のそれぞれは、コンピュータプログラムとして実現される。当該プログラムは、ICカード100のROMに格納され実行されるものと、外部よりダウンロードされ、FeRAM202に格納され実行されるものとがある。

[0221] (実施の形態1～4の第2の補足事項)

また、さらに、上述の電圧検出部300等の機能ブロックは、CPU、RAM、ROM、不揮発性メモリ等のハードウェア資源との組み合わせにより、集積回路であるLSIとして実現される場合がある。これらは、個別に1チップ化されても良いし、一部又はすべてを含むように1チップ化されても良い。

[0222] 図22は、実施の形態1のICカード100における集積回路化の一例を示す図である。LSI1600は集積回路化の一例を示し、集積回路化する機能ブロックの範囲の例である。ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

[0223] また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製作後にプログラムすることが可能なField Programmable Gate Array(FPGA)やLSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

[0224] さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて機能ブロックの集積化を行なってもよい。バイオ技術、有機化学技術等の適用が可能性としてありえる。

[0225] また、実施の形態2～実施の形態4のICカード100のそれぞれにおいても、それらが有する機能ブロックの一部または全部を集積回路化することができる。

産業上の利用可能性

[0226] 本発明の半導体メモリカードは、プログラムを実行可能な機能を有する半導体メモリカードとして有用である。特に複数のプログラムを実行可能なICカードとして有用である。

請求の範囲

[1] プログラムを実行可能な半導体メモリカードであって、

情報を格納する不揮発性メモリと、

実行中のプログラムに関する情報を格納するレジスタと、

前記半導体メモリカードに対する供給電圧の変化を検出する検出部と、

前記検出部が所定の電圧低下状態を検出した場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避部と、

前記検出部が所定の電圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰部と

を備える半導体メモリカード。

[2] 更に、他の機器と通信する通信部を備え、

前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記付加情報が、前記通信部と前記他の機器との通信により得られた情報を含むとき、前記レジスタ情報を前記レジスタに復帰させる

請求項1記載の半導体メモリカード。

[3] 更に、前記通信部と前記他の機器との通信における通信種別を示す情報を取得する通信種別取得部を備え、

前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記付加情報が、前記通信種別取得部により取得された前記通信種別を示す情報を含むとき、前記レジスタ情報を前記レジスタに復帰させる

請求項2記載の半導体メモリカード。

[4] 前記不揮発性メモリは、互いに異なる複数のレジスタ情報を格納し、

前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記通信種別取得部により取得された前記通信種別を示す情報を含む付加情報に対応付けられたレジスタ情報を、前記不揮発性メモリの中から選択して読み出し、前記レジスタに復帰させる

請求項3記載の半導体メモリカード。

[5] 前記退避部は、前記レジスタ情報を前記不揮発性メモリに退避させる際に、更に、前記プログラムが利用する暗号の強度を示す暗号情報を前記レジスタ情報と対応付けて前記不揮発性メモリに退避させ、

前記半導体メモリカードは、更に、

他の機器と通信する通信部と、

前記復帰部が前記レジスタ情報を前記レジスタに復帰させる前に、前記暗号情報に示される暗号の強度が所定の強度以上であるか否かを判断する復帰判断部と、

前記復帰判断部が、前記暗号情報に示される暗号の強度が所定の強度以上であると判断した場合、前記他の機器の認証を行なう認証部とを備え、

前記復帰部は、前記検出部が所定の電圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たし、かつ、前記認証部による前記他の機器の認証が成功したとき、前記レジスタ情報を前記レジスタに復帰させる

請求項1記載の半導体メモリカード。

[6] 前記不揮発性メモリは破壊読出し領域を有し、

前記半導体メモリカードは、更に、前記退避部が前記レジスタ情報を前記レジスタに退避させる前に、実行中のプログラムが利用する暗号の強度が所定の強度以上であるか否かを判断する退避判断部を備え、

前記退避部は、前記検出部が所定の電圧低下状態を検出した場合、前記退避判断部により前記暗号の強度が所定の強度以上であると判断されたとき、前記レジスタ情報と前記付加情報とを対応付けて前記不揮発性メモリの前記破壊読出し領域に退避させる

請求項1記載の半導体メモリカード。

[7] 前記不揮発性メモリは、Ferroelectric Random Access Memory(FeRAM)である

請求項6記載の半導体メモリカード。

[8] プログラムを実行可能な半導体メモリカードにおいて前記プログラムを断続的に実

行するためのプログラム実行方法であって、

前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のプログラムに関する情報を格納するレジスタとを有し、

前記プログラム実行方法は、

前記半導体メモリカードに対する供給電圧の変化を検出する検出ステップと、

前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、

前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップと

を含むプログラム実行方法。

[9] アプリケーションプログラムを実行可能な半導体メモリカードにおいて前記アプリケーションプログラムを断続的に実行するための実行プログラムであって、

前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のアプリケーションプログラムに関する情報を格納するレジスタとを有し、

前記実行プログラムは、

前記半導体メモリカードに対する供給電圧の変化を検出する検出ステップと、

前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記アプリケーションプログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、

前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップと

をコンピュータに実行させるための実行プログラム。

[10] アプリケーションプログラムを実行可能な半導体メモリカードにおいて前記アプリケーションプログラムを断続的に実行するための実行プログラムが格納された、コンピュ

ータが読み取り可能な記録媒体であって、

前記半導体メモリカードは、情報を格納する不揮発性メモリと、実行中のアプリケーションプログラムに関する情報を格納するレジスタとを有し、

前記記録媒体は、

前記半導体メモリカードに対する供給電圧の変化を検出する検出ステップと、

前記検出ステップにおいて、所定の電圧低下状態が検出された場合、前記レジスタに格納されている情報であるレジスタ情報と、前記アプリケーションプログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避ステップと、

前記検出ステップにおいて、所定の電圧上昇状態が検出された場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰ステップと

をコンピュータに実行させるための実行プログラムが格納された記録媒体。

[11] プログラムを実行可能な半導体メモリカードにおいてプログラムを断続的に実行するための集積回路であって、

前記半導体メモリカードは、情報を格納する不揮発性メモリが設けられており、

前記集積回路は、

実行中のプログラムに関する情報を格納するレジスタと、

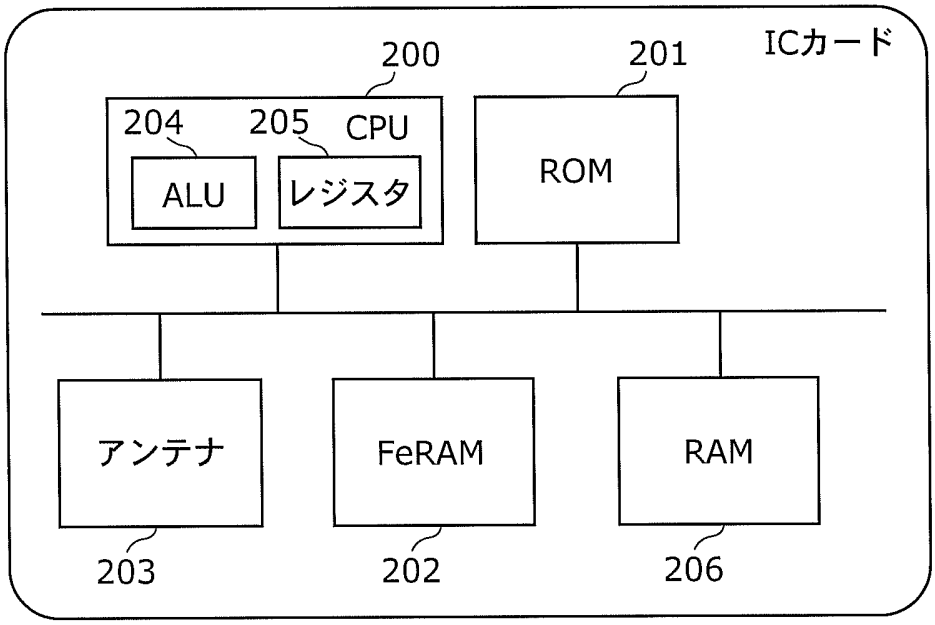
前記半導体メモリカードに対する供給電圧の変化を検出する検出部と、

前記検出部が所定の電圧低下状態を検出した場合、前記レジスタに格納されている情報であるレジスタ情報と、前記プログラムを特定するための付加情報とを対応付けて前記不揮発性メモリに退避させる退避部と、

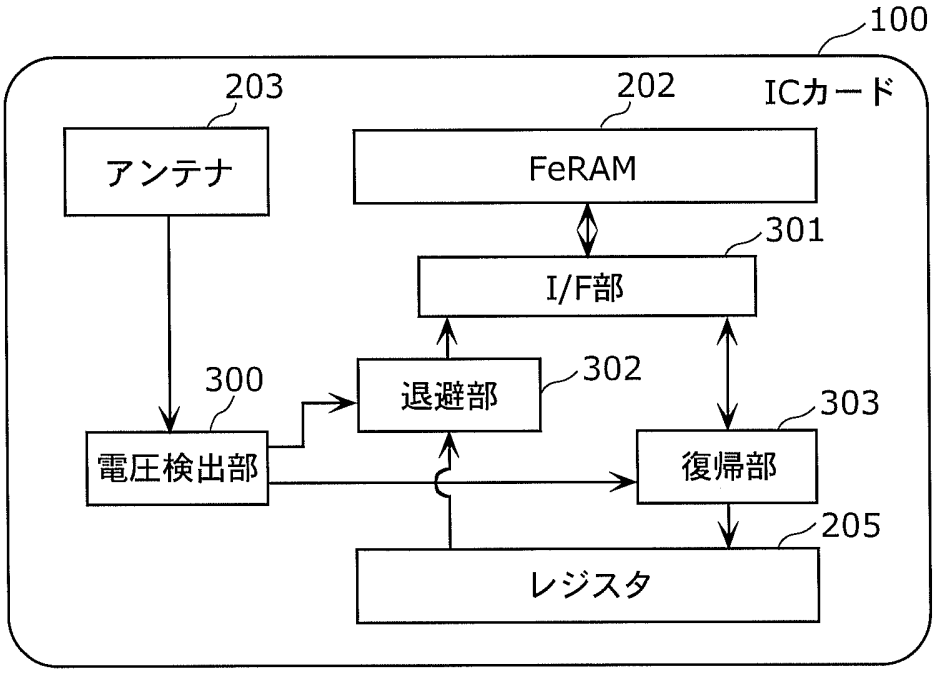
前記検出部が所定の電圧上昇状態を検出した場合、前記不揮発性メモリに格納されている前記付加情報が所定の条件を満たすとき、前記レジスタ情報を前記レジスタに復帰させる復帰部と

を備える集積回路。

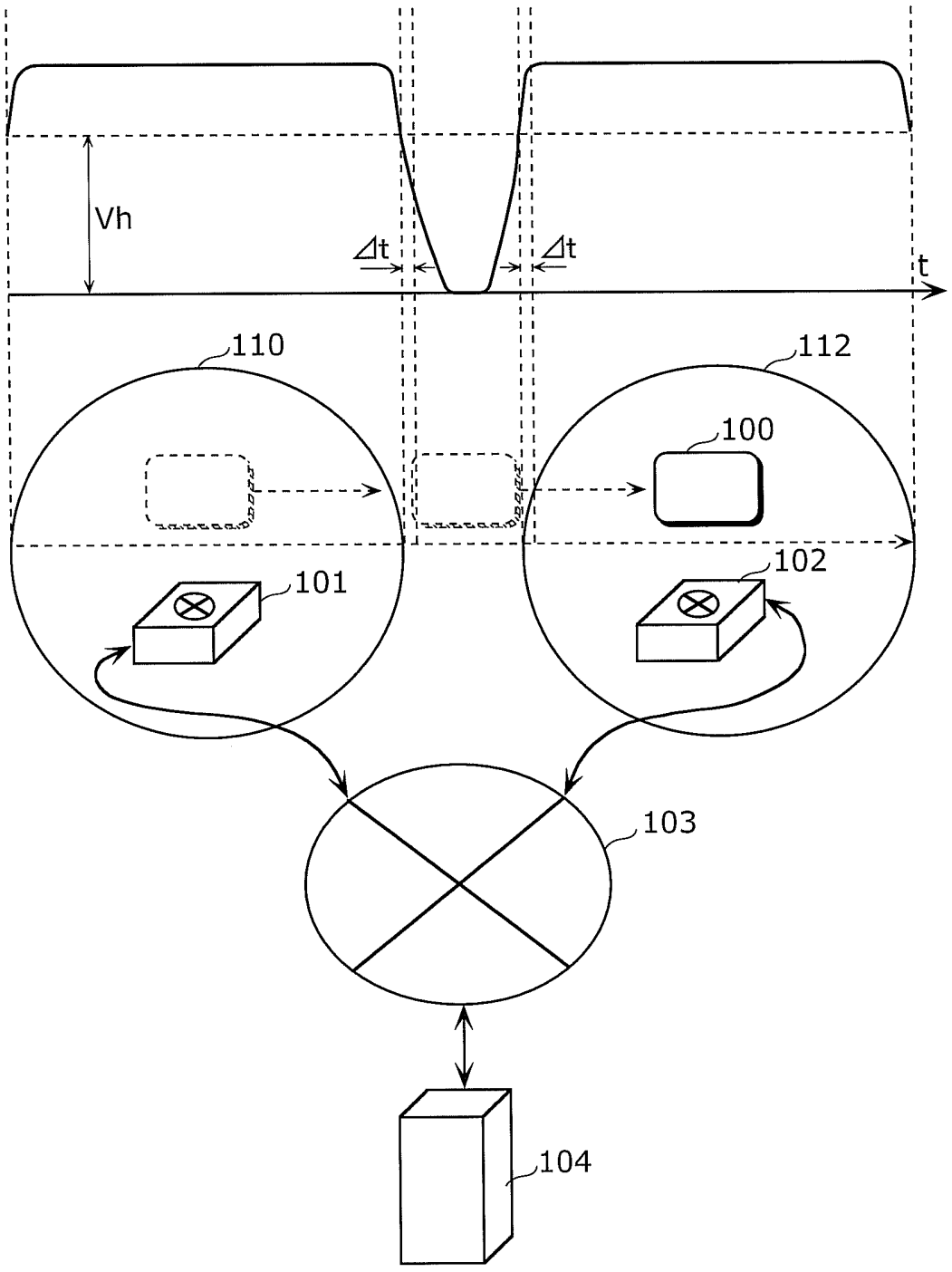
[図1]


ICカード
200
201
204
205
CPU
ALU
レジスタ
ROM
アンテナ
FeRAM
RAM
203
202
206

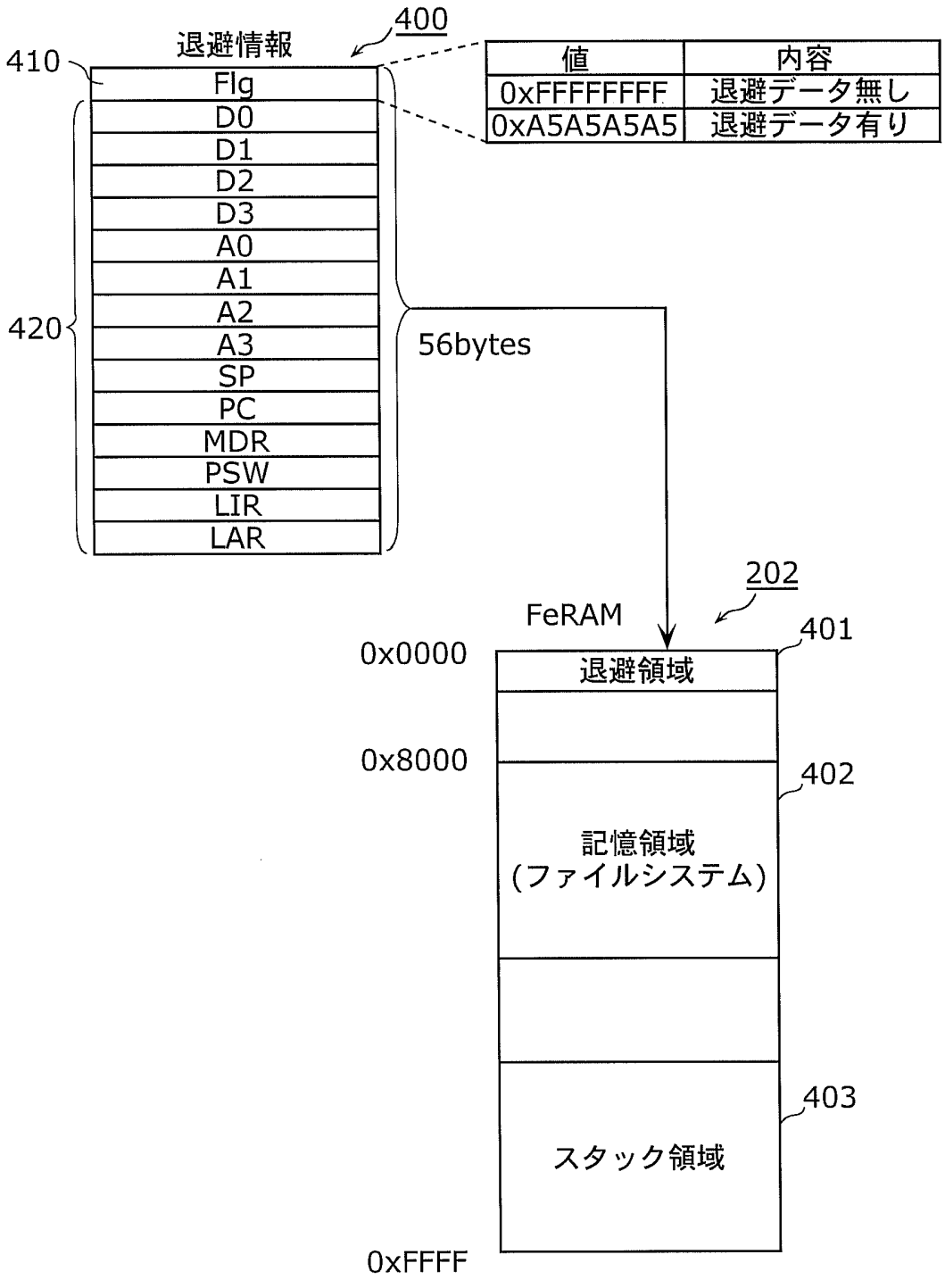
[図2]


100
ICカード
203
202
アンテナ
FeRAM
301
I/F部
300
退避部
302
303
電圧検出部
復帰部
205
レジスタ

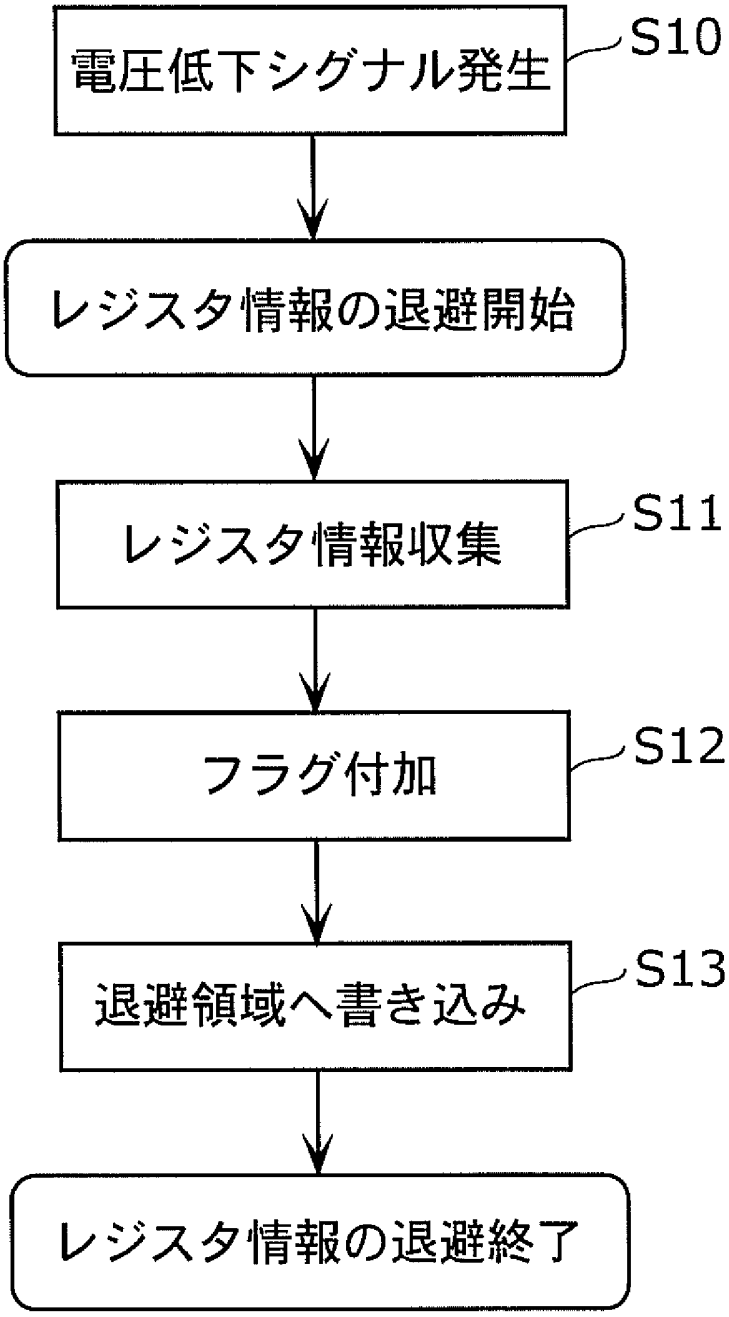
[図3]



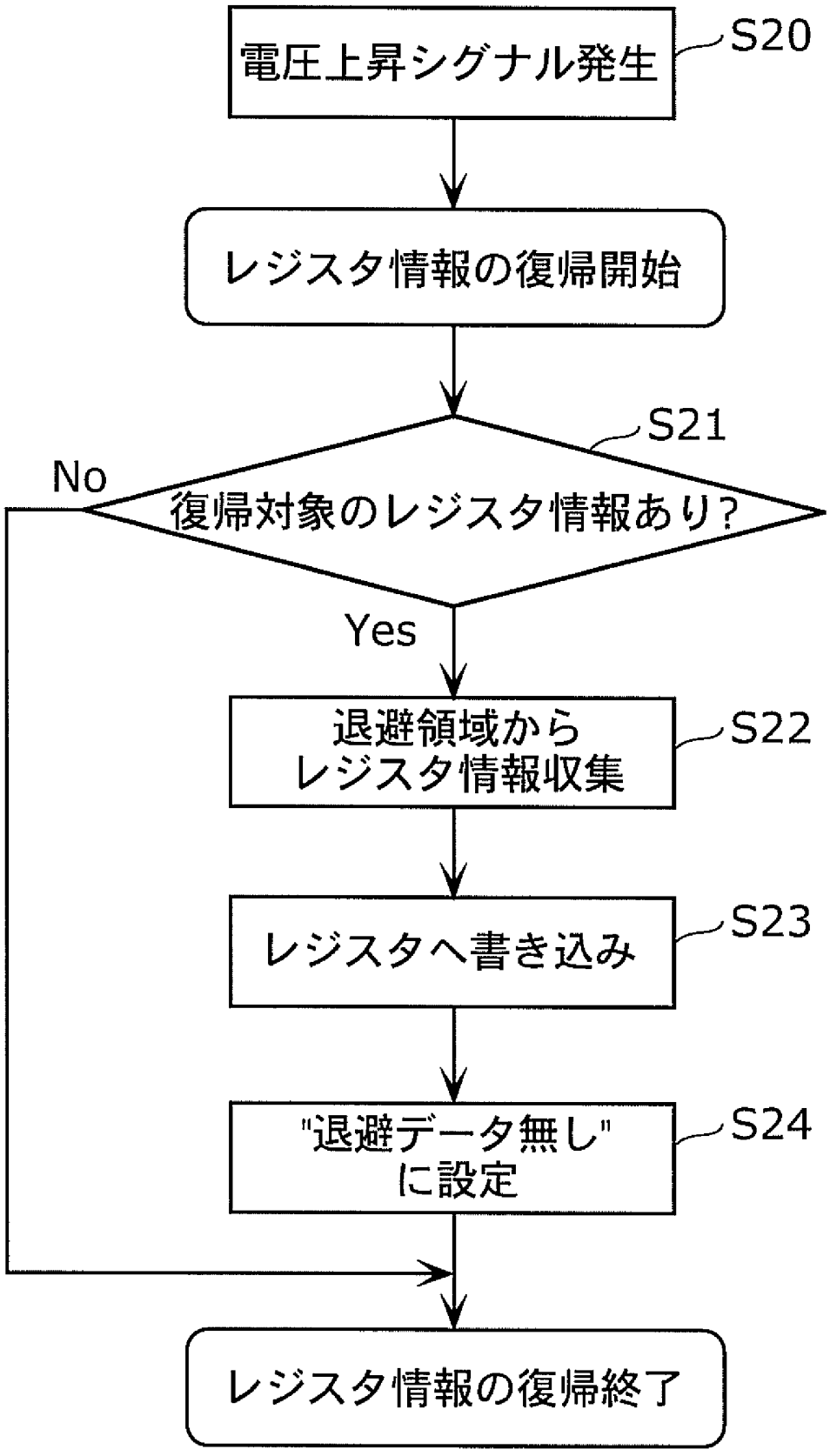
[図4]


400
退避情報
410
Flg
D0
D1
D2
D3
A0
A1
A2
A3
SP
PC
MDR
PSW
LIR
LAR
420
56bytes
値
内容
0xFFFFFFFF
退避データ無し
0xA5A5A5A5
退避データ有り
202
FeRAM
401
0x0000
退避領域
0x8000
402
記憶領域
(ファイルシステム)
403
スタック領域
0xFFFF

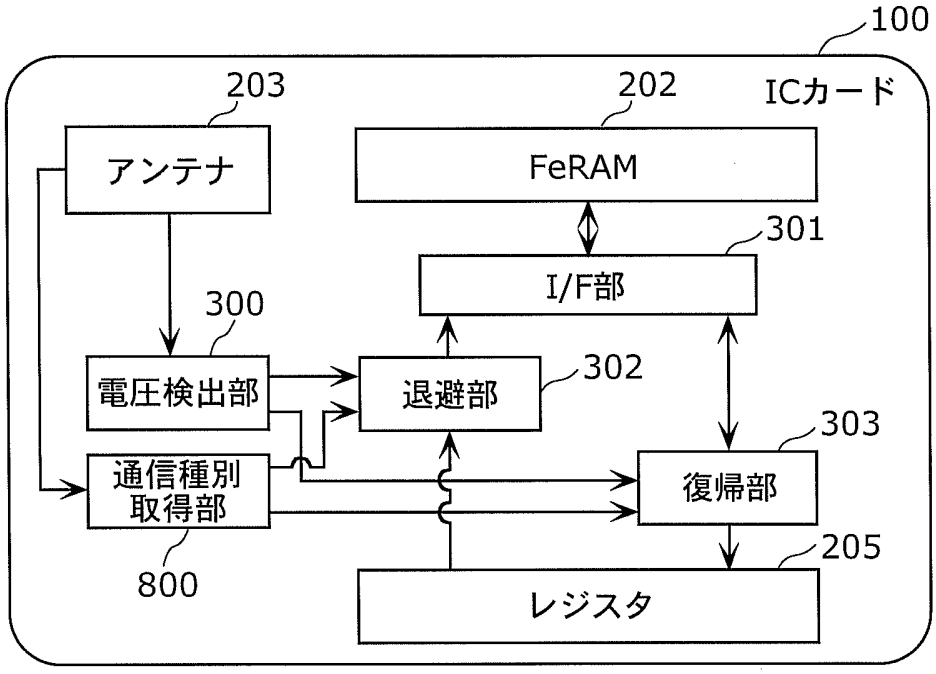
[図5]


電圧低下シグナル発生
S10
レジスタ情報の退避開始
レジスタ情報収集
S11
フラグ付加
S12
退避領域へ書き込み
S13
レジスタ情報の退避終了

[図6]


電圧上昇シグナル発生
S20
レジスタ情報の復帰開始
S21
No
復帰対象のレジスタ情報あり?
Yes
退避領域から
レジスタ情報収集
S22
レジスタへ書き込み
S23
"退避データ無し"
に設定
S24
レジスタ情報の復帰終了

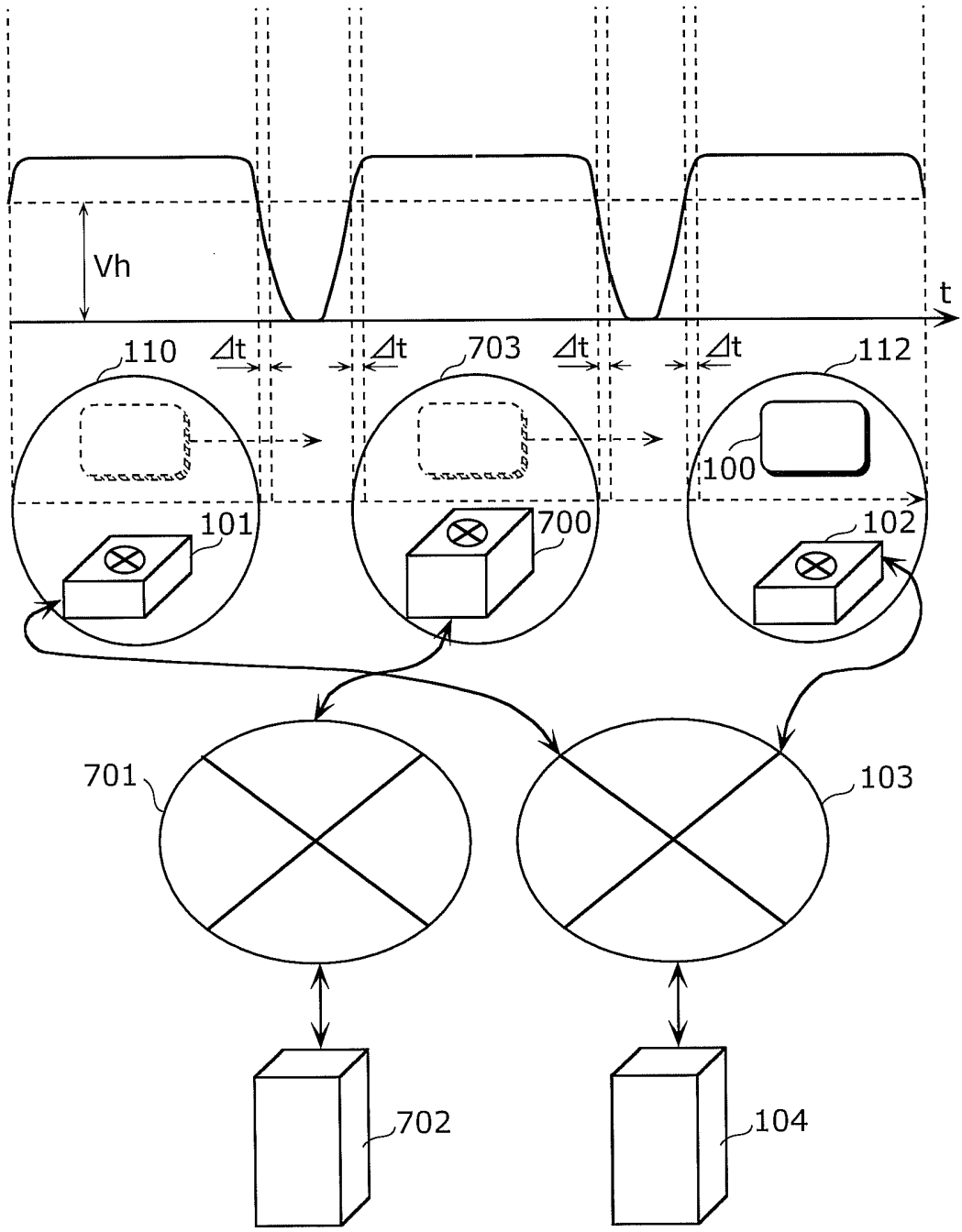
[図7]



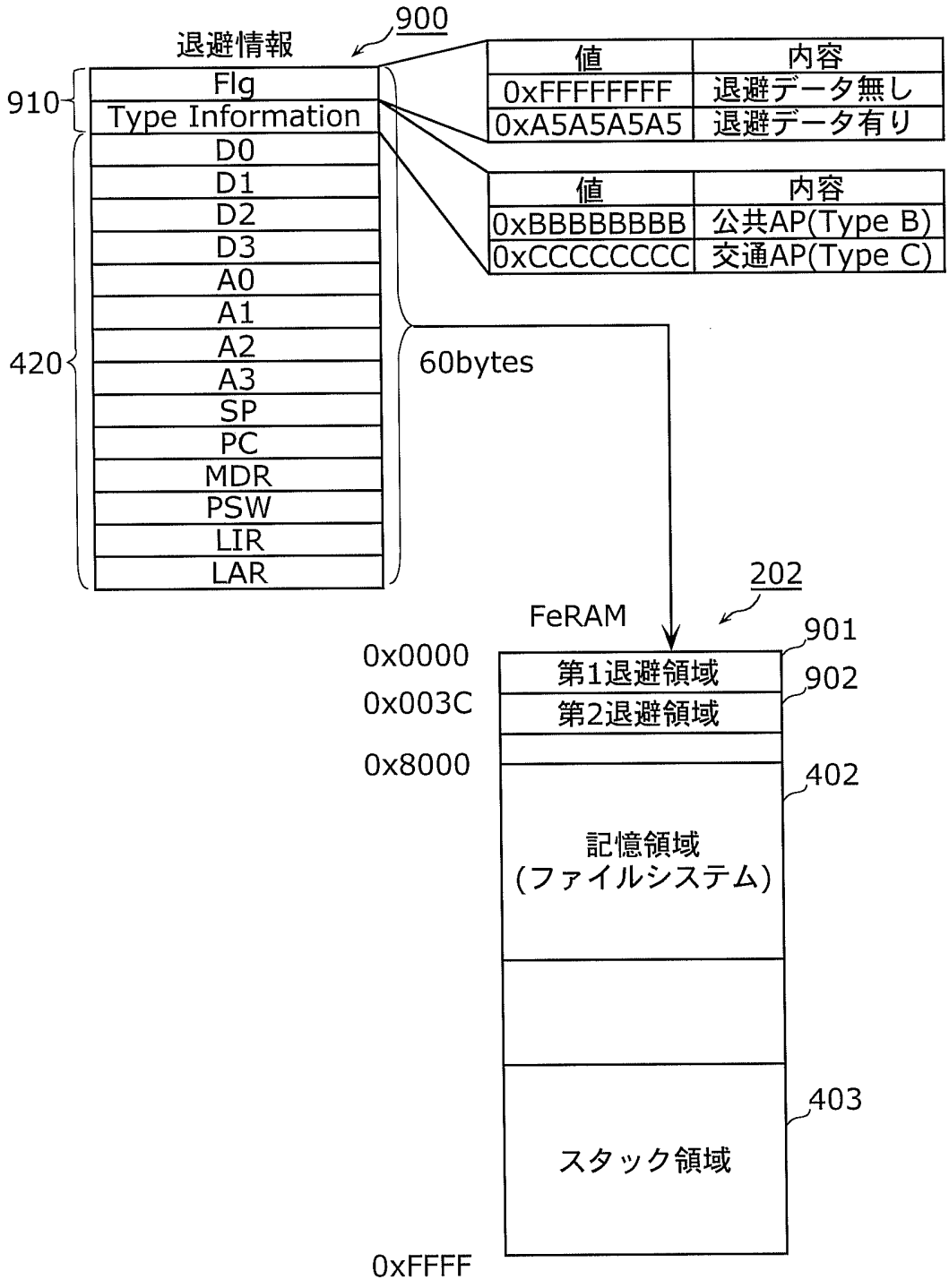
[図8]

Transport Type		
項目	値	説明
Type_A	0x0010	TypeA
Type_B	0x0020	TypeB
Type_C	0x0030	TypeC
Reserved future use	0x0040-0x00FF	予約済
Reserved	0x0100-0xFFFF	予約済

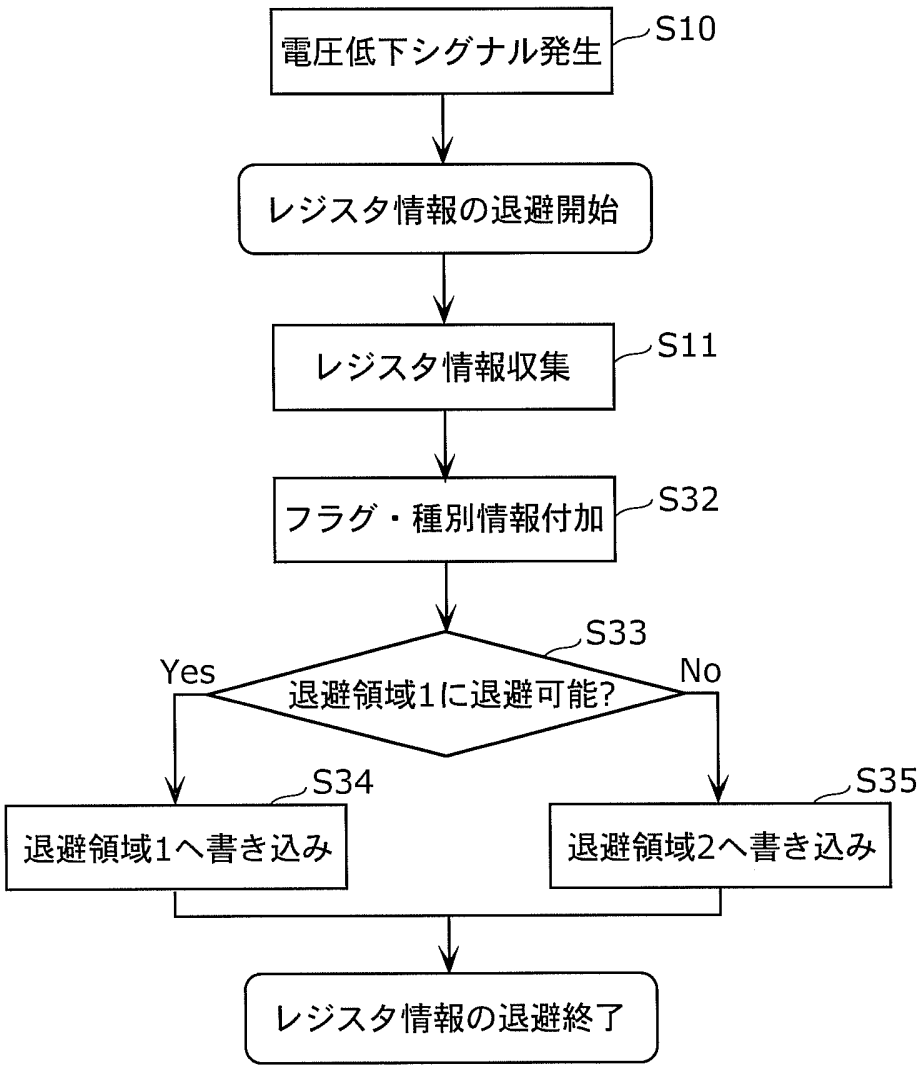
[図9]



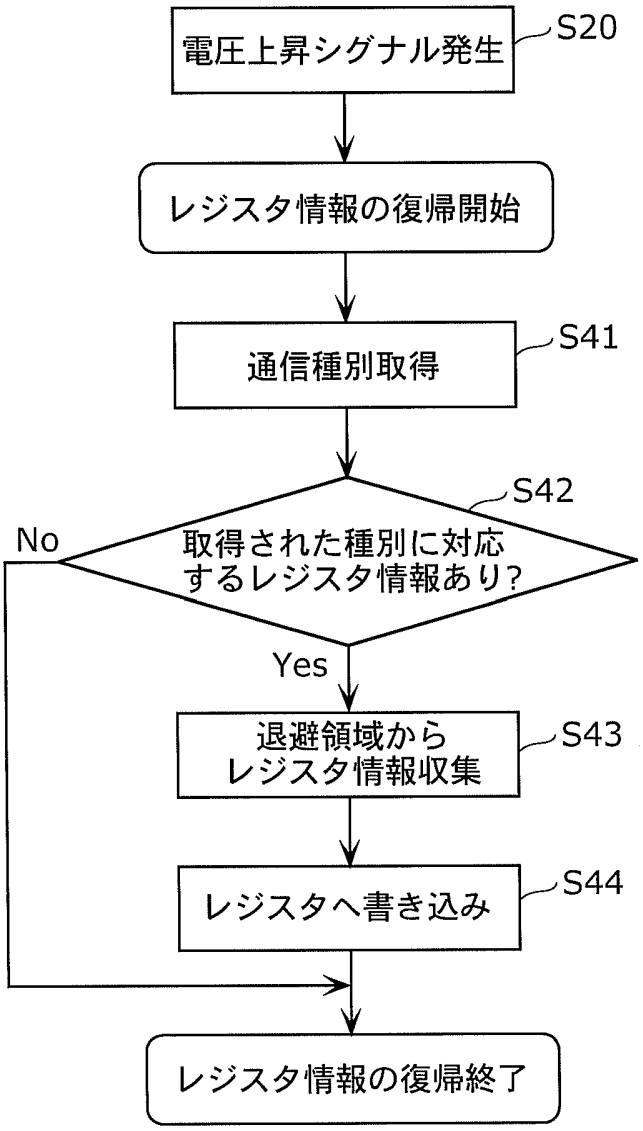
[図10]


900
退避情報
910
Flg
Type Information
D0
D1
D2
D3
A0
A1
A2
A3
SP
PC
MDR
PSW
LIR
LAR
420
値
内容
0xFFFFFFFF
退避データ無し
0xA5A5A5A5
退避データ有り
値
内容
0xBBBBBBBB
公共AP(Type B)
0xCCCCCCCC
交通AP(Type C)
60bytes
202
FeRAM
901
902
402
403
0x0000
0x003C
0x8000
0xFFFF
第1退避領域
第2退避領域
記憶領域
(ファイルシステム)
スタック領域

[図11]


電圧低下シグナル発生
S10
レジスタ情報の退避開始
レジスタ情報収集
S11
フラグ・種別情報付加
S32
S33
Yes
退避領域1に退避可能?
No
S34
退避領域1へ書き込み
S35
退避領域2へ書き込み
レジスタ情報の退避終了

[図12]

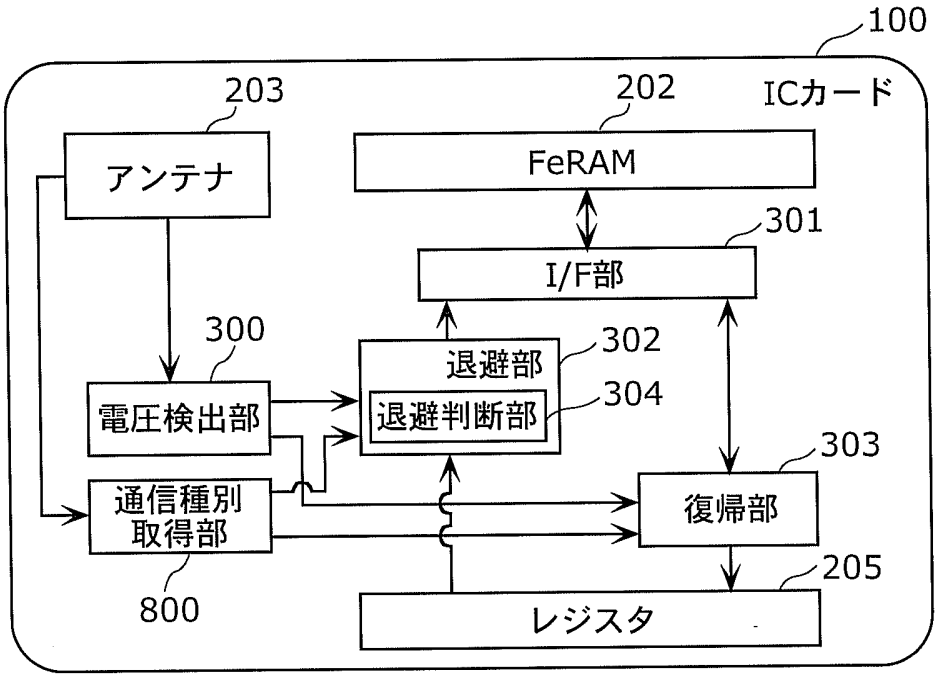

電圧上昇シグナル発生
S20
レジスタ情報の復帰開始
通信種別取得
S41
S42
No
取得された種別に対応するレジスタ情報あり?
Yes
退避領域からレジスタ情報収集
S43
レジスタへ書き込み
S44
レジスタ情報の復帰終了

[図13]

付加情報の例

項目	サイズ (byte)	型	説明
Resume Version	4	DWORD	Resume Version
Application ID	4	DWORD	アプリケーション識別子
Application Type	2	WORD	アプリケーション種別 (RESUME, CA_RESUME, etc...)
Transport Type	2	WORD	通信プロトコル (TYPE_B, TYPE_C, etc...)
Transport info length	4	DWORD	通信プロトコル長
Transport Information	Transport info length	Tsinfo	通信プロトコル情報

[図14]



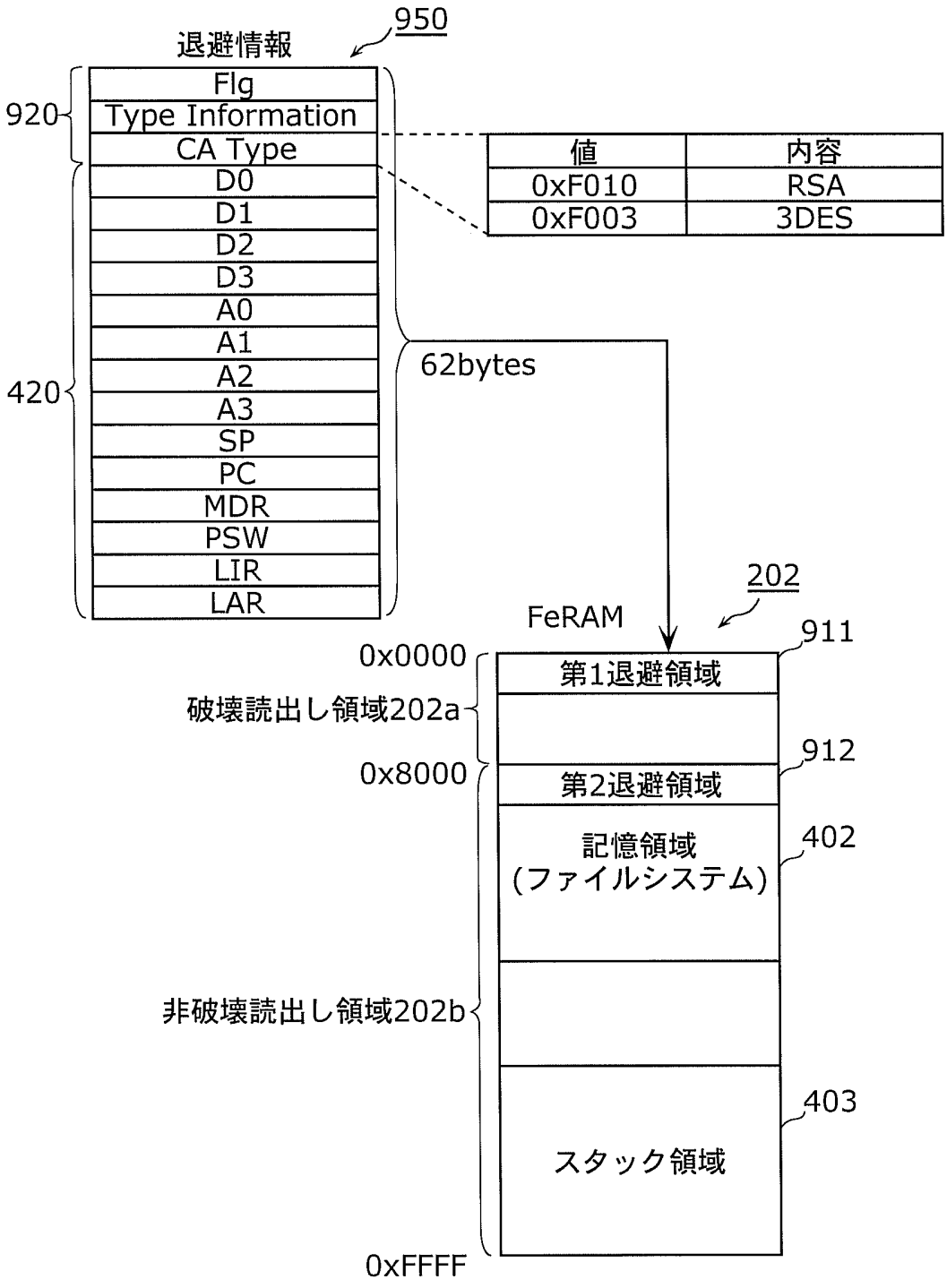
[図15]

CA情報			
項目	サイズ (byte)	型	説明
CA Type	2	WORD	CA種別
CA Key length	4	DWORD	鍵長
CA Key	CA Key length	CAKey	鍵情報

[図16]

CA Type		
項目	値	説明
NO_USE	0x0000	暗号化なし
M_CA_DES	0xF001	Single DES
M_CA_3DES	0xF003	3 DES
M_CA_RSA	0xF010	RSA
Reserved		予約済

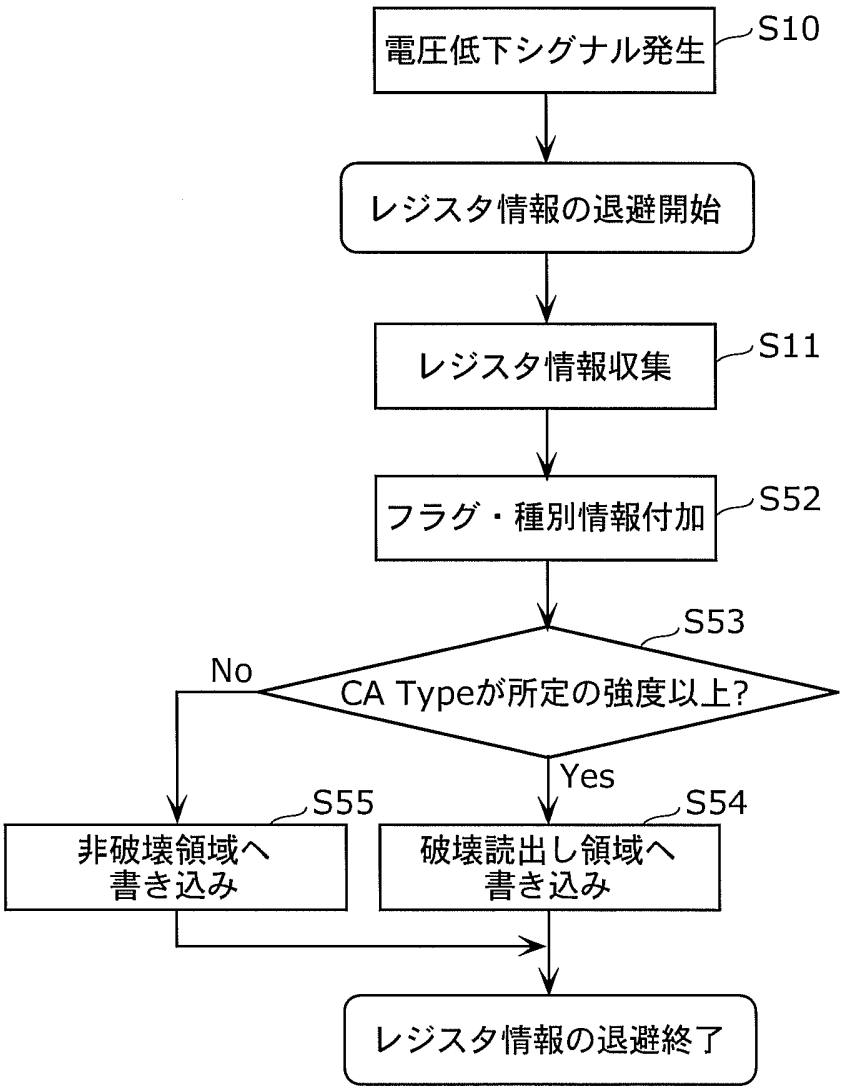
[図17]


950
退避情報
920
Flg
Type Information
CA Type
D0
D1
D2
D3
A0
A1
A2
A3
SP
PC
MDR
PSW
LIR
LAR
420
値
内容
0xF010
RSA
0xF003
3DES
62bytes
202
FeRAM
911
0x0000
第1退避領域
破壊読出し領域202a
912
0x8000
第2退避領域
記憶領域
(ファイルシステム)
402
非破壊読出し領域202b
403
スタック領域
0xFFFF

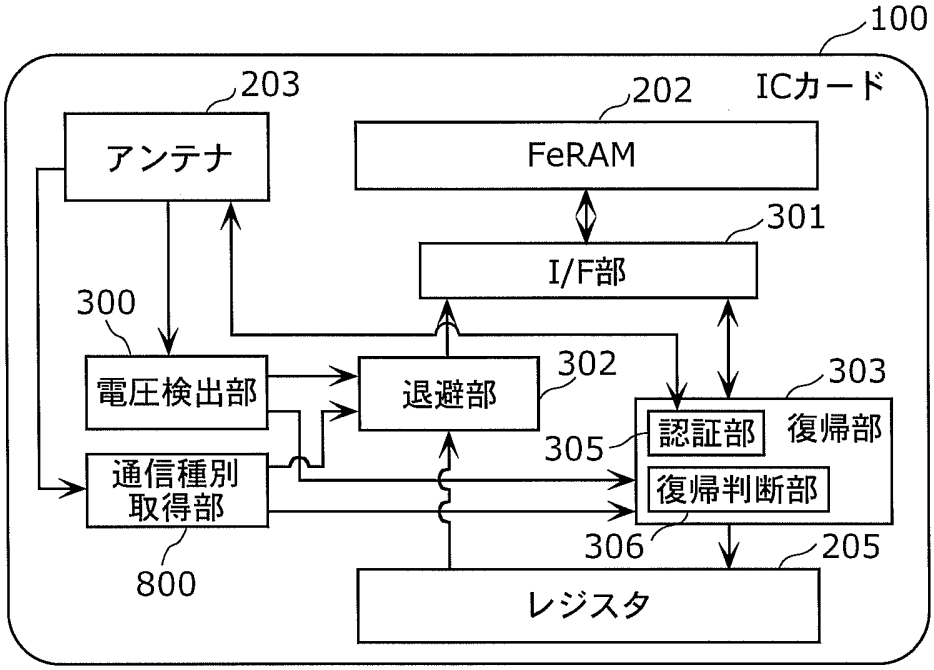
[図18]

アドレス	領域
最上位ビット 0 0x0000～0x7FFF	破壊読出し
最上位ビット 1 0x8000～0xFFFF	非破壊読出し

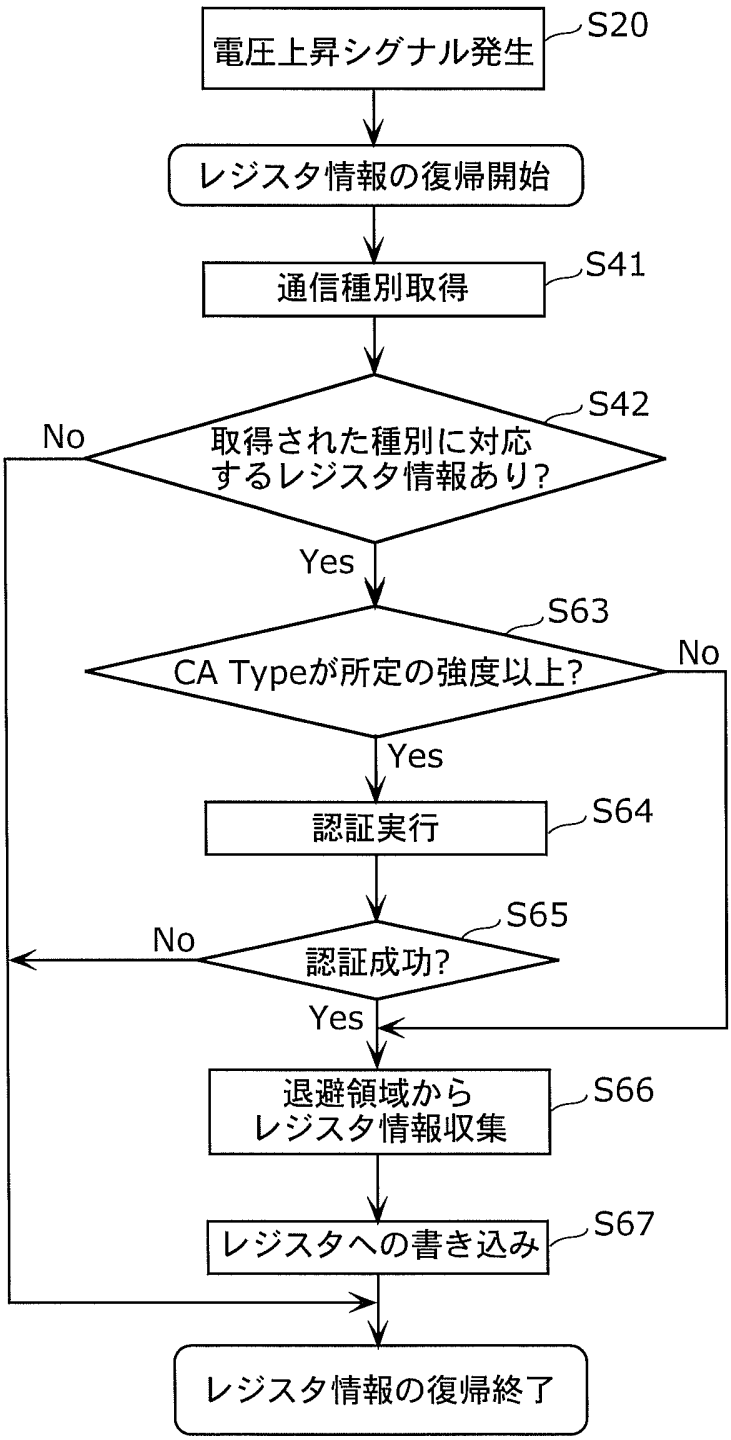
[図19]



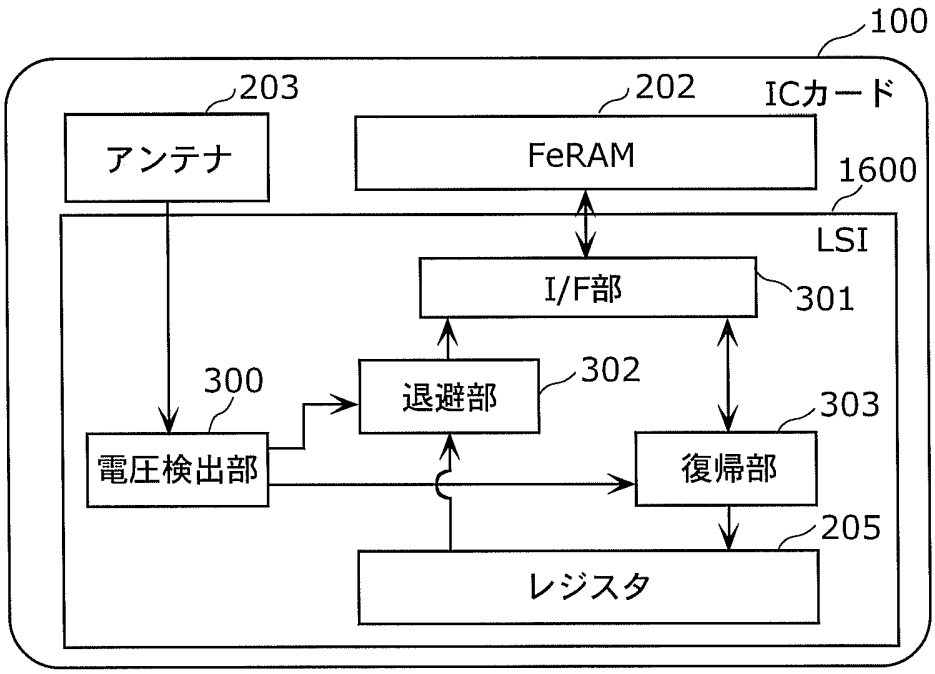
[図20]


100
ICカード
203
アンテナ
202
FeRAM
301
I/F部
300
電圧検出部
退避部
302
303
認証部
復帰部
305
通信種別
取得部
復帰判断部
306
205
800
レジスタ

[図21]


電圧上昇シグナル発生
S20
レジスタ情報の復帰開始
通信種別取得
S41
取得された種別に対応するレジスタ情報あり?
S42
No
Yes
CA Typeが所定の強度以上?
S63
No
Yes
認証実行
S64
認証成功?
S65
No
Yes
退避領域からレジスタ情報収集
S66
レジスタへの書き込み
S67
レジスタ情報の復帰終了

[図22]


100
ICカード
203
アンテナ
202
FeRAM
1600
LSI
I/F部
301
300
退避部
302
303
電圧検出部
復帰部
205
レジスタ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/016849

A. CLASSIFICATION OF SUBJECT MATTER
G06K19/07 (2006.01), ***G06F1/30*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K19/07 (2006.01), ***G06F1/30*** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2003-122648 A (Matsushita Electric Industrial Co., Ltd.), 25 April, 2003 (25.04.03), Full text; all drawings & US 2003-095463 A1	1,8-11 2-4 5-7
Y A	JP 3-111954 A (NEC Corp.), 13 May, 1991 (13.05.91), Full text; all drawings (Family: none)	2-4 5-7
Y A	JP 2-234260 A (Sony Corp.), 17 September, 1990 (17.09.90), Full text; all drawings (Family: none)	2-4 5-7

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 October, 2005 (14.10.05)	25 October, 2005 (25.10.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０１６８４９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　***G06K19/07*** (2006.01), ***G06F1/30*** (2006.01)

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　***G06K19/07*** (2006.01), ***G06F1/30*** (2006.01)

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y A	JP 2003-122648 A (松下電器産業株式会社) 2003.04.25, 全文、全図 & US 2003-095463 A1	1,8-11 2-4 5-7
Y A	JP 3-111954 A (日本電気株式会社) 1991.05.13, 全文、全図 (ファミリーなし)	2-4 5-7
Y A	JP 2-234260 A (ソニー株式会社) 1990.09.17, 全文、全図 (ファミリーなし)	2-4 5-7

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１４．１０．２００５	２５．１０．２００５

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5N	8320
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	丹治　彰 電話番号　０３－３５８１－１１０１　内線　３５８６		